Deploying and configuring Avaya Agent for Desktop

Release 2.0.6.14
Issue 1
July 2021

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License 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

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.

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 Inc.

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

Contents

Chapter 1: Introduction

Purpose

This document describes how to install, configure, and uninstall Avaya Agent for Desktop.

.

Change history

The following table describes the changes made in this document for each release:

Issue	Date	Summary of changes
1, Release 2.0.6	August, 2020	The following sections are updated: • Interoperability • Port requirements • Audio requirements - supported headsets • New in this release • DNS server configuration • AADS support overview • AADS server configuration • Enabling AADS login settings in Avaya Agent for Desktop • Server menu field descriptions • Avaya Workspaces for Elite Supported Scenarios • Avaya Oceana™ Workspaces supported scenarios • Software requirements • Hardware requirements • Topology • List of supported Avaya Agent for Desktop settings on AADS • Key Strokes menu field descriptions • Configuring Avaya Agent for Desktop for using SIP shared control mode • Configuring Avaya Agent for Desktop for using SIP shared control mode with J179 hardphone • Configuring the connection to a SIP proxy server • Configuring the WebLM license URL for H.323 and SIP • Configuring the connection to Avaya Aura® Communication Manager • Configuring the connection to Avaya Control Manager
2, Release 2.0.6.7	Dec, 2020	The updates are as follows: • AADS parameter "3RD_PARTY_CERT_MODE" is renamed to "THIRD_PARTY_CERT_MODE". • The topic 'Session Manager survivability for SIP signaling' is added. • Avaya Aura®Device Services (AADS) content is restructured and new content is added. • Chapters 2 and 3 is restructured.

Table continues…

Issue	Date	Summary of changes
3, Release 2.0.6.11	March, 2021	The updates are as follows: • Linux installation procedures are added. • The guide is re-structured. • Instructions and extra information about the configuration of feature buttons are added in the following topics in Chapter 5: - Installation and configuration - Assigning functions to buttons in Avaya Aura® Communication Manager - Assigning functions to buttons for SIP users in Avaya Aura® System Manager. • In the section Audio Requirements, headsets are segregated into groups. 'Extended' is changed to 'Advanced', according to the user interface. • New parameters are added in Chapter 7: Settings configuration. • A new chapter on Security is added.
4, Release 2.0.6.12	April, 2021	The updates are as follows: • The diagram in the topic 'Deployment process' is replaced by text. • Usage scenario diagrams are moved into different sections. • A new topic 'Functions of Aux Work Reason codes' is added in Chapter 8. • More information is added about parameters and reason codes.
5, Release 2.0.6.13	June, 2021	The updates are as follows: • A new topic Using No Hold Type of conference is added in Settings configuration. • A new topic Downgrading Avaya Agent for Desktop is added in Installation and configuration. • The list of parameters is updated. • The Lock Manager section is updated. • The chapter Security is updated.

Table continues…

Issue	Date	Summary of changes
6, Release 2.0.6.14		The updates are as follows: • A new topic is Configuring the WiFi infrastructure is added in Overview. • A new topic Network configurations and diagnostics is added in Overview. • A new chapter PCN and PSN notifications is added. • The topic Desktop Platform security recommendations is added in Security.. • The topic No transference of sensitive data is added in Security. • The topic Supported cipher suites is edited. • New parameters are added.

Intended audience

This document is intended for the personnel who deploy and configure Avaya Agent for Desktop at a customer site.

Section 508 Compliance support

Avaya Agent for Desktop graphical user interface is now largely compliant with the relevant Section 508 standards. Testing is complete on most of these features using JAWS for Windows 10 64-bit (JAWS 2019.1907.42 Offline 64-bit August 2019).

For users who are visually challenged and using screen reader software, the most accurate compliance score is "Supports when Combined with Compatible Assistive Technology". Avaya Agent for Desktop is based on a Qt framework. Support for Qt-based applications by assistive technologies is improving but is currently incomplete. Accessibility support in Qt consists of a generic interface, implemented for technologies on each platform: MSAA on Windows, Mac OS X accessibility on the Mac, and Unix/X11 AT-SPI on Linux. Accessibility interface of Qt closely follows the Microsoft Active Accessibility (MSAA) standard, which is supported by most clients. Other technologies used by Qt provide similar functionality.

For users who have low vision, the most accurate compliance score is "Supports with Exceptions". Avaya Agent for Desktop uses a custom scheme of colors and fonts that cannot be changed by the user. This fixed set of colors and fonts may be problematic for some users with low vision. The use of screen magnification software is supported, and most of these products have features that let the user override the colors of the application and enlarge the fonts. For keyboard-only usage, Avaya Agent for Desktop offers enhanced keyboard commands using Key Strokes configuration settings to control the application. Visually challenged users can also access all controls of Avaya

Agent for Desktop using the "Tab' key. Users must refer to the available documentation for Avaya Agent for Desktop 2.0.x for more details.

Note:

SSB BART Group did not audit Avaya Agent for Desktop's requirements in § 1194.21, § 1194.22, § 1194.23, and § 1194.24. The § 1194.21, § 1194.22, § 1194.23, and § 1194.24 audit of Avaya Agent for Desktop was performed by Avaya and the results are reported in a separate VPAT.

Related Resources

Documentation

The following table lists the documents related to Avaya Agent for Desktop. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Using		
Using Avaya Agent for Desktop	Provides information about using Avaya Agent for Desktop product features and functions.	Technical support representatives and authorized business partners
Administration		
Administering Network Connectivity on Avaya Aura® Communication Manager	Provides information about configuring and administering network components of Avaya Aura® Communication Manager.	Technical support representatives and authorized business partners
Deploying Avaya Workspaces for Elite guide	Provides information about installation, configuration, and administration procedures for Avaya Workspaces for Elite.	Technical support representatives and authorized business partners
Administering Avaya Aura® Call Center Elite	Provides information about administering Automatic Call Distribution (ACD) and Call Vectoring features.	Implementation engineers and system administrators.

Table continues…

Title	Description	Audience
Avaya Application Solutions: IP Telephony Deployment Guide	Provides information about Avaya's Application Solutions product line, IP Telephony product deployment, and network requirements for integrating IP Telephony products with an IP network. The guide can be used as a tool to provide a better understanding of the benefits of Avaya IP solutions and of the many aspects of deploying IP Telephony on a customer's data network.	Implementation engineers, support personnel, sales engineers, and business partners
Avaya Aura® Communication Manager Network Region Configuration Guide	The intent of this guide is to provide training on Avaya Aura® Communication Manager network regions, and to give guidelines for configuring them.	Implementation engineers, support personnel, sales engineers, and business partners
Avaya Aura® Communication Manager Survivability Options	Provides information about installing and configuring survivable core server.	Technical support representatives and authorized business partners
Administering Avaya Aura® Session Manager	Provides information about administering and managing Avaya Aura® Session Manager.	Implementation engineers, support personnel, sales engineers, and business partners
Administering Avaya Session Border Controller for Enterprise	Provides information about administering and managing Avaya Session Border Controller for Enterprise.	Technical support representatives and authorized business partners
Configuring Avaya Control Manager	Provides information about configuring Avaya Control Manager.	Technical support representatives and authorized business partners
Administering Avaya Control Manager for Avaya one-X® Agent Central Management	Provides information about administering the functioning of Avaya Control Manager for Avaya one-X ® Agent Central Management.	Technical support representatives and authorized business partners
Administering Avaya Aura® Device Services	Administering Avaya Aura® Device Services.	System administrators, support personnel
Administering Avaya Aura® Session Manager	Administer the Session Manager interface.	System administrators, support personnel

Chapter 2: Overview

Avaya Agent for Desktop overview

Avaya Agent for Desktop is a client application for contact centers. An agent can use Avaya Agent for Desktop for handling incoming and outgoing calls, changing work states, and managing other UI controls. However, only an administrator can manage the configurations and settings of the application.

Avaya Agent for Desktop supports multiple platforms and is designed to function in the following use cases:

- **Virtual Desktop Infrastructure (VDI):** Avaya Agent for Desktop provides a solution to deliver real-time media with VDI support in Citrix and VMware Horizon environments on HP and Dell based thin clients running on Windows and Linux based operating systems. An administrator can use Avaya Agent for Desktop for VDI to enable desktop virtualization that encompasses the hardware and software systems required to support the virtualized environment in a contact center.
- **Standalone Contact Center Client:** Avaya Agent for Desktop provides a full set of features for a contact center agent and can be used as a primary client application on Windows, Mac and Linux operating systems.

Avaya Agent for Desktop uses Avaya Aura® Communication Manager to store station configuration settings and manage agent profiles locally. You can also choose to use Avaya Control Manager for managing agent profiles.

New features in 2.0.6.13 release

No new features are added in this release. For details about sections updated in this guide, see *Change history*.

Deployment process

About this task

This is an overview of the deployment process for Avaya Agent for Desktop.

Procedure

1. Planning and preconfiguration:
    a. Complete the customer site survey.
    b. Complete the site preparation.
    c. Obtain the appropriate components and licenses used for Avaya Agent for Desktop .
2. Initial setup and connectivity:
    a. Set up the required hardware components.
    b. Install the operating system and required software.
    c. Configure the network.
    d. Download Avaya Agent for Desktop installer.
3. Installation:
    a. Configure FTP servers. This is used for thin client distribution.
    b. Install Avaya Agent for Desktop .
4. Configuration:
    a. Configure Communication Manager.
    b. Confgure SBC settings.
    c. Configure Avaya Agent for Desktop .
    d. Check the network's quality of service (QoS).

Topology

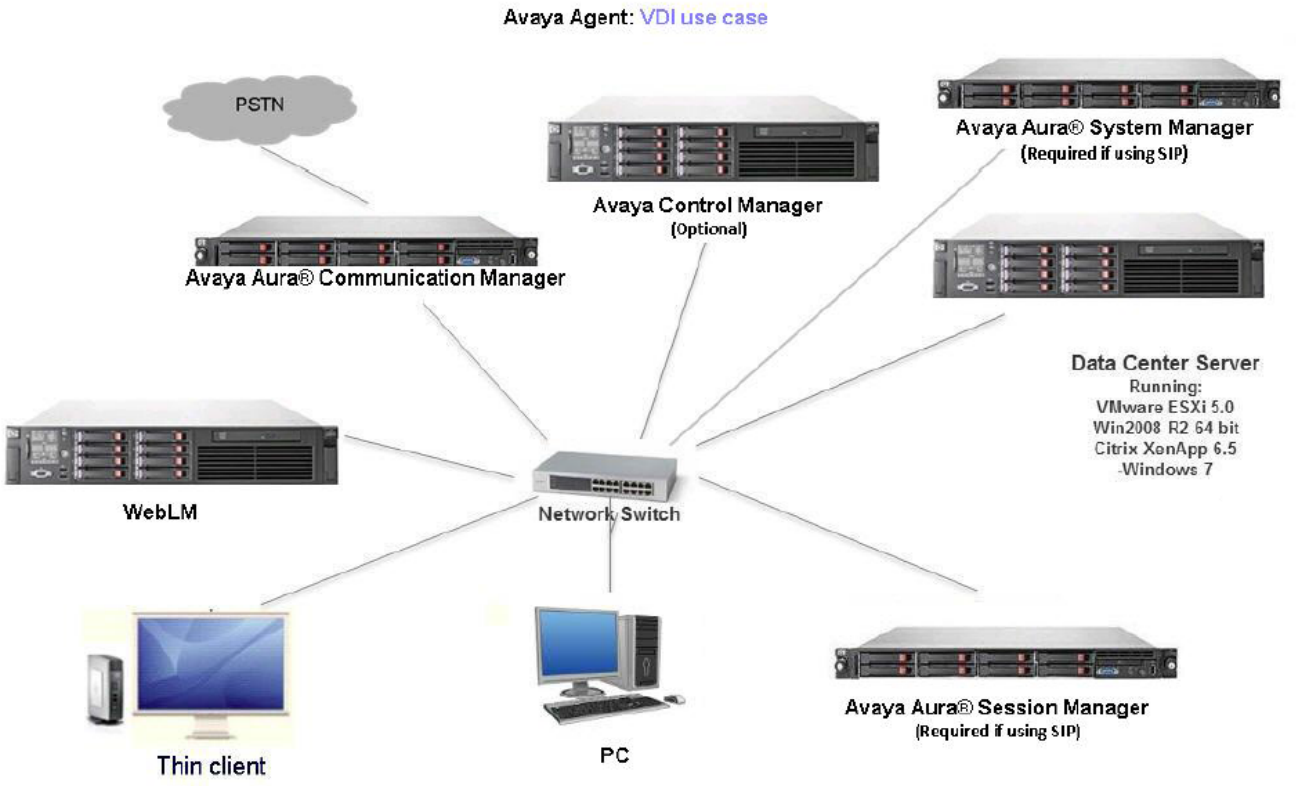


Figure 1: Avaya Agent for Desktop topology diagram: VDIA use case

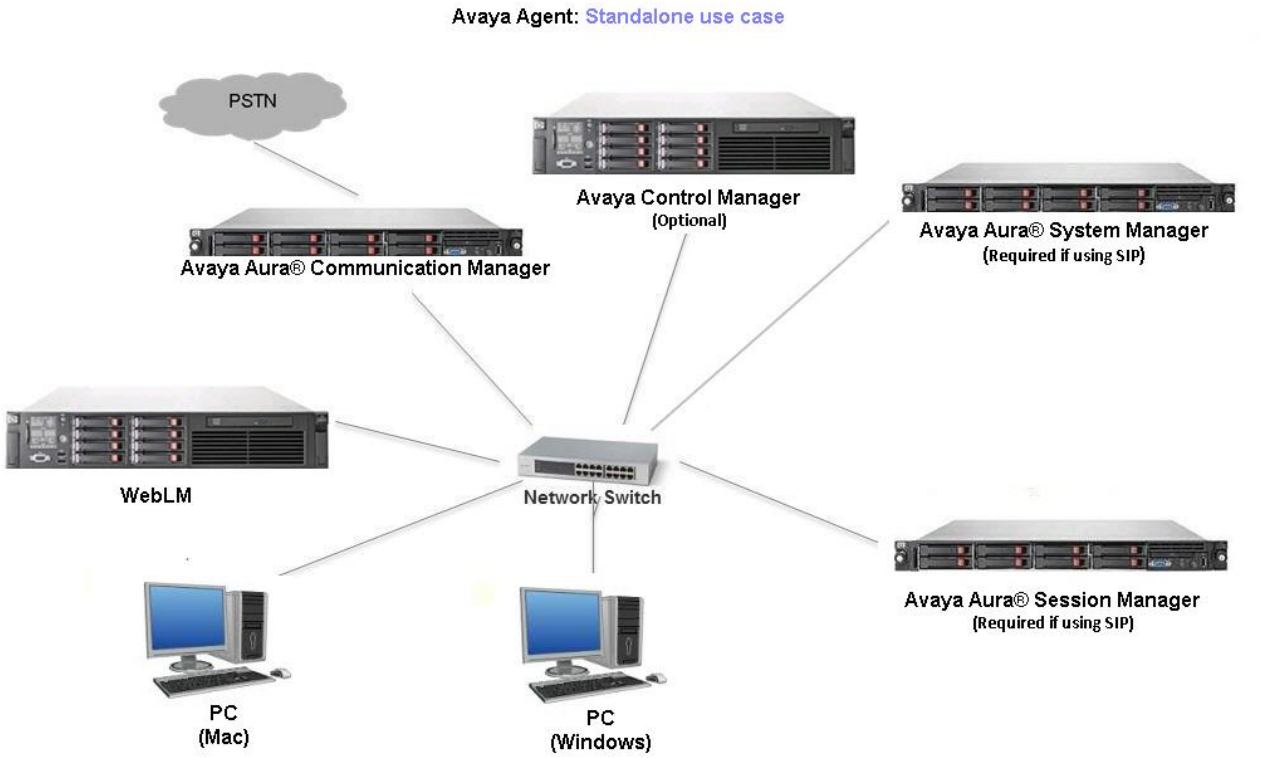


Figure 2: Avaya Agent for Desktop topology diagram: Standalone use case

Table 1: Components of the Avaya Agent for Desktop architecture

Component	Description
Avaya Aura® 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.
Avaya Control Manager	Avaya Control Manager is a centralized operational administration solution that enables contact center administrators and supervisors to control all of the administrative elements that comprise a single or multiple location Avaya-based contact center environment. Contact center users, agents and other entities can be managed from a single Web-based user interface and provisioned across a range of Avaya applications in a contact center environment.

Table continues…

Component	Description
Avaya Aura® Device Services	With Avaya Aura® Device Services, you can roll out multiple clients and seamlessly transition between devices. Avaya Aura® Device Services acts as a single point of administration for endpoints. It can also provide file server capabilities, such as firmware and settings files. Avaya Aura® Device Services can handle traditional IP phones, such as the 96xx Series Phones, and the complex configuration of SIP endpoints, such as Avaya Workplace Client.
Avaya Aura® System Manager	Avaya Aura® System Manager is a central management system that provides a set of shared management services and a common console. Avaya Aura® System Manager also provides the capability to upgrade, migrate, and install software patches for Avaya Aura applications.
Avaya Aura® Session Manager	Avaya Aura® Session Manager is the core of Avaya's Session Initiated Protocol (SIP) based architecture. The Session Manager platform makes it possible to unify media, networks, devices, applications and real-time, actionable presence across a common infrastructure, creating the on-demand access to services and applications that define the engagement experience.
WebLM	The server used for Avaya Agent for Desktop licensing.
PC	Personal computer to deploy Avaya Agent for Desktop standalone application.
Data Center Server	The virtualization server that hosts the PC capabilities of the thin clients.

Hardware requirements

Avaya Agent for Desktop for VDI can be deployed on the following thin clients:

Supported thin clients	details
HP thin clients	HP T530 Win 10 IOT and HP T530 ThinPro 6.x HP T620 (Windows 10) HP T630 (Windows 10) and HP T630 (Windows 10 IOT) HP T730 (ThinPro 7.2 64 bit) IGEL (Windows 10)

The agent workstations that run Avaya Agent for Desktop as a standalone application must have the following system configuration:

- Processor: 1.5 GHz or higher
- HDD: 10 GB or higher
- RAM: 1 GB or higher
- A compatible audio device for input and output

Note:

Without a local audio device Avaya Agent for Desktop does not work.

Avaya Agent for Desktop supports the following station types:

Protocol	Supported station type
H.323	9650, 4620, 9640, 9641, 9608, 9621, and 9611. **Note:** For H.323 shared control mode when Avaya Agent for Desktop is in desk phone mode with J1XX series phones, you must use the station type 96x1 only.
SIP	9650 SIPCC, 9608 SIPCC, 9641 SIPCC, 9621 SIPCC, 9611 SIPCC and J179CC. **Note:** For SIP shared control mode when Avaya Agent for Desktop is in desk phone mode with Avaya one-X® Agent, you must use station type as 9608SIPCC only.

Software requirements

Operating Systems Requirements

The agent workstations that run Avaya Agent for Desktop must have one of the following operating systems installed:

- Microsoft Windows 10 64-bit and 32-bit
- MacOS 10.14 and 10.15
- OSS8

You can install Avaya Agent for Desktop for VDI on multiple agent stations by using Wyse Device Manager (WDM) for the Dell Wyse clients or HP Device Manager (HPDM) for the HP clients.

The Device Manager software provides management, configuration, monitoring, and protection functions for multiple endpoints in a distributed computing environment.

The system requirements for Wyse Device Manager are:

Operating system	• Windows Server 2008 R2 (64-bit) • Windows Server 2008 R2 Service Pack 1 (64-bit)
Database server	• Microsoft SQL Server 2005 • Microsoft SQL Server 2005 Express • Microsoft SQL Server 2008 • Microsoft SQL Server 2008 Express • Microsoft SQL Server 2008 R2 Express (32–bit)

The system requirements for HP Device Manager are :

Operating system	• Windows 2000 Server Service Pack 4 • Windows 2003 Server Service Pack 2 • Windows Server 2008 R2 (64-bit)
Database server	• Microsoft SQL Server 2000 • Microsoft SQL Server 2005 • Microsoft SQL Server 2008 • PostgreSQL
Third-party software	Oracle Java Runtime Environment, version 6 update 2

Other supported operating systems:

- Apple macOS: 10.14 Mojave, 10.15 Catalina and 11 Big Sur
- IGEL Universal Management Suite (UMS) 5

Browser Requirements (for click to dial feature)

Operating Systems/ Browsers	Windows	Mac OS	Linux with RPM based packages	Linux with DEB based packages
Embedded browser	Supported	Supported	Supported	Supported
Google Chrome version 65 or above	Supported	Supported	Not supported	Not supported
Mozilla Firefox	Not supported	Not supported	Not supported	Not supported
Safari	Not supported	Not supported	Not supported	Not supported
Internet Explorer	Not supported	Not supported	Not supported	Not supported
Microsoft Edge	Not supported	Not supported	Not supported	Not supported

While using Avaya Agent for Desktop, Avaya recommends you to have the latest manufacturer recommended patches, updates, and device drivers for the best experience.

Network requirements

Using a program that relies on VoIP technology requires increased network resources and performance optimizations, because VoIP requires dedicated bandwidth and is easily affected by network problems.

You must perform a network assessment before installing Avaya Agent for Desktop, so that performance and stability issues do not affect Avaya Agent for Desktop.

The network assessment services for Avaya VoIP consist of the following phases:

- Basic Network Assessment: a high-level LAN/WAN infrastructure evaluation that determines the suitability of an existing network for VoIP.
- Detailed Network Assessment: the second phase in the Network Assessment for IP Telephony solutions.

The detailed network assessment takes information gathered in the basic network assessment, performs problem diagnosis, and provides functional requirements for the network to implement Avaya VoIP.

The voice over IP network readiness assessment evaluates the state of a customer's network infrastructure to ascertain whether the infrastructure can support voice over IP traffic.

Avaya requires evidence that a customer's network infrastructure meets the network requirements by conducting a voice over IP.

Network readiness assessment is a precondition to deployment and/or support of all solutions that include delivery of voice communications using transmission of Internet Protocol (IP).

Metric	Recommended	Acceptable
One-way network delay	< 80 milliseconds	< 180 milliseconds
Network jitter	< 10 milliseconds	< 20 milliseconds
Network packet loss (Voice)	1.0%	3.0%
Network Packet Loss (Video)	0.1%	0.2%
QoS Enabled	Required	Required

To confirm compliance with the Network requirements, customer must timely provide Avaya with a completed Network Readiness Assessment Results document ("Compliance Evidence"). The Compliance Evidence warrants that customer's network complies with the Network Requirements and acknowledges that Avaya:

- May rely on the Compliance Evidence
- Does not validate the Compliance Evidence
- Is not responsible for ensuring Customer's compliance with the Network requirements.

For more information about network assessments, see:

- *"Network assessment offer" in Avaya Application Solutions: IP Telephony Deployment Guide, 555-245-600*.
- Avaya Professional Services (APS).

Avaya Professional Services (APS) supports a portfolio of consulting and engineering offers to help plan and design voice and data networks, including:

- IP Telephony
- Data Networking Services
- Network Security Services

You can contact Avaya CSI:

- On the Web: http://csi.avaya.com/
- By email: bcsius@avaya.com
- By phone: +1 866 282 9266

See http://netassess.avaya.com for a description of the Avaya network assessment policy. This link is available only from within the Avaya corporate network.

Voice Quality of Service (QoS)

Avaya Agent for Desktop supports the Layer 3 Differentiated Services Code Point (DiffServ). Avaya Agent for Desktop does not support the Resources ReSerVation Protocol (RSVP) or the Layer 2 QoS: 802.1p/Q mechanism. Avaya Agent for Desktop retrieves the QoS DiffServ values from the associated network region displayed the registration confirmation message from Avaya Aura® Communication Manager.

For more information, see *Chapter 5: Voice and Network Quality* in *Administration in Administering Network Connectivity on Avaya Aura™ Communication Manager, 555-233-504 Issue 14 May 2009*.

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 Agent for Desktop 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 for Enterprise 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 Agent for Desktop 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

For troubleshooting issues, it may be necessary to report logs to your support organization. Logging for Avaya Agent for Desktop 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.

Best practices for WiFi

Avaya Agent for Desktop can be used over ethernet or WiFi. Following are the best practices and prerequisites:

- 4.8, 5 or 5.9GHz WiFi is more stable than 2.4 or 3.6 GHz, as they are less susceptible to interference. However, 4.8, 5 or 5.9GHz WiFi has a shorter range.
- Mobile phone 'hotspots' are not a WiFi alternative.

Changes in the networking and device adapters during a call is not supported. The following active call scenarios may result in a call drop:

- If the workstation is docked or undocked.
- Switching between ethernet and WiFi, or vice-versa.
- If the VPN gets disconnected or reconnected, or both.
- If the workstation's local IP address changes.

Configuring the WiFi infrastructure

About this task

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

Procedure

1. For a home WiFi router, use the latest firmware for the device in accordance with the instructions of the manufacturer.
2. For an enterprise-class Wi-\Fi security switch, ensure that the switch uses the latest software release.
3. If you change the configuration, you must remove the WiFi settings from your network for any device that connects to your WiFi router.
4. When you remove the WiFi 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.
5. For applications that use a WiFi security switch or router:
   a. Establish a VLAN for traffic use on your new Service Set Identifier (SSID).
   b. Configure the new VLAN with dedicated bandwidth control on Session Manager.
   c. 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 WiFi switches or routers.
6. Disable hidden networks.

   Hidden networks do not broadcast the SSID. Your device may not be able to easily detect the hidden network, resulting in increased connection time and reduced reliability of automatic connections.
7. 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.

8. Set your security mode as follows:
    a. Set security to the WPA2 mode, known as AES.

       AES is the strongest form of security that WiFi products offer.

    b. When you enable WPA2, choose a strong password based on your enterprise guidelines.
9. 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 WiFi router does not support the WPA/WPA2 mode.
10. Disable 40 MHz in the 2.4 GHz settings on the WiFi router to reduce interference issues.
11. Disable lower speeds, such as, 1, 2, and 5.5 Mbps, and do the following:
    a. Change 6 Mbps to Mandatory and the beacon rate to 6 Mbps.
    b. Set multicast to Automatic.
    c. Set all other rates to **Supported**. This setting might be unavailable on a home WiFi router.

Port requirements

Avaya Agent for Desktop Port Matrix

Source		Destination		Network or Application protocol	Traffic purpose	Comment
Initiator	**Ports**	**Receiver**	**Ports**			
Avaya Agent for Desktop	Ephemeral	Avaya Control Manager	80	HTTP	Avaya Control Manager	You can configure port for this in Avaya Control Manager.
Avaya Agent for Desktop	Ephemeral	Avaya Control Manager	443	HTTPS	Secure Avaya Control Manager	You can configure port for this in Avaya Control Manager.
Avaya Agent for Desktop	Ephemeral	Avaya Aura® Session Manager	80	HTTP	PPM	

Table continues…

Source		Destination		Network or Application protocol	Traffic purpose	Comment
Initiator	Ports	Receiver	Ports			
Avaya Agent for Desktop	Ephemeral	Avaya Aura® Session Manager	443	HTTPS	Secure PPM	
Avaya Agent for Desktop	Ephemeral	WebLM	52233	HTTPS	WebLM	You can configure port for this in WebLM.
Avaya Agent for Desktop	Ephemeral	Avaya Aura® Session Manager	5060	UDP	SIP	Unsecured SIP Signaling
Avaya Agent for Desktop	Ephemeral	Avaya Aura® Session Manager	5060	TCP	SIP	Unsecured SIP Signaling
Avaya Agent for Desktop	Ephemeral	Avaya Aura® Session Manager	5061	TLS	SIP	Secure SIP Signalling
Avaya Agent for Desktop	Ephemeral	Avaya Aura® Communication Manager	1719	UDP	H323 – H225 Registration	
Avaya Aura® Communication Manager	61440	Avaya Agent for Desktop	1024 or 13926	TCP	H323 – H225 Signaling	TTS enabled
Avaya Agent for Desktop	1024 or 13926	Avaya Aura® Communication Manager	61440	TCP	H323 – H225 Signaling	TTS disabled
Avaya Agent for Desktop	Ephemeral	Far end Endpoint	2050–3329	UDP	Media with SIP	You can configure port for this inAvaya Aura® Communication Manager.
Avaya Agent for Desktop	2070	Far end Endpoint	2050–3329	UDP	Media with H323	You can configure port for this in Avaya Aura® Communication Manager.

Table continues…

Source		Destination		Network or Application protocol	Traffic purpose	Comment
Initiator	Ports	Receiver	Ports			
Avaya Agent for Desktop	Ephemeral	LDAP Server	389	TCP	LDAP	You can configure port for this in LDAP server.
Avaya Agent for Desktop	Ephemeral	LDAP Server	636	TLS	Secure LDAP	You can configure port for this in LDAP server.
Avaya Agent for Desktop	Ephemeral	Syslog Server	514	UDP	Syslog (Remote logging)	
Avaya Agent for Desktop	Ephemeral	AADS	443	HTTPS	AADS auto configuration service	You can configure port for this service on AADS
Avaya Agent for Desktop	Ephemeral	Prognosis	5005	TCP	RTCP Monitoring	RTCP Monitoring through Prognosis

WebLM requirements

Supported release	WebLM standalone application **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 vitual)	10,000

Audio requirements

Audio codecs:

Avaya Agent for Desktop supports the following audio codecs:

- G.711A and G.711MU
- G.729 and G.729A

The audio codecs are configured on the Avaya Aura® Communication Manager side, in the IP Codecs Set section.

For **Headset Integration**, Avaya Agent for Desktop has the following:

- **Voice**: Avaya Agent for Desktop supports only audio with headsets. Call control is not supported with Voice.
- **Basic**: You can select only one call control from the options of **Answer**, **Hold** and **Drop**. An agent can perform call controlling with the headset.

  Example: If you select **Hold**, then **Answer** and **Drop** do not work. Only that selected call control works.
- **Advanced**: All call controls supported by the vendor headset including mute, unmute, and headset volume adjustment are supported with Advanced or Basic.

Note:

Some headsets do not support some specific call controls. Example, a type of headset does not support mute and unmute. Another type of headset supports only hold and drop, but does not support answer.

Supported headsets:

Table 2: Avaya headsets

Headset / Adaptor	Windows AAfD 32-bit (exe)	Windows AAfD 64-bit (exe)	ThinPro, Debian, Ubuntu AAfD 32-bit and 64-bit (deb)	RedHat SUSE Linux AAfD 32-bit and 64-bit (rpm)	MacOS AAfD 64-bit (dmg)
Avaya L139 headset (Avaya L100 Controller)	Voice	Voice	Voice	Voice	Voice
Avaya L159 USB	Voice	Voice	Voice	Voice	Basic
Avaya L139 with L100 USB Adapters HID	Voice	Voice	Voice	Voice	Basic

Table 3: Jabra headsets

Headset / Adaptor	Windows AAfD 32-bit (exe)	Windows AAfD 64-bit (exe)	ThinPro, Debian, Ubuntu AAfD 32-bit and 64-bit (deb)	RedHat SUSE Linux AAfD 32-bit and 64-bit (rpm)	MacOS AAfD 64-bit (dmg)
Jabra link 280	Voice	Voice	Voice	Voice	Voice
Jabra link 220	Voice	Voice	Voice	Voice	Voice
Jabra BIZ 2300	Advanced	Advanced	Basic	Basic	Advanced
Jabra Evolve 40 ENC010 USB	Advanced	Advanced	Basic	Basic	Advanced
Jabra BIZ 2400 II USB	Advanced	Advanced	Basic	Basic	Advanced
Jabra Evolve 40 UC Mono USB	Advanced	Advanced	Basic	Basic	Advanced
Jabra Evolve 65 Link 370	Advanced	Advanced	Voice	Voice	Voice
Jabra Evolve 75 Link 370	Advanced	Advanced	Voice	Voice	Voice
Jabra Evolve2 65 Link 380	Advanced	Advanced	Voice	Voice	Voice
Jabra Engage 50	Advanced	Advanced	Voice	Voice	Voice

Table 4: Plantronics headsets

Headset / Adaptor	Windows AAfD 32-bit (exe)	Windows AAfD 64-bit (exe)	ThinPro, Debian, Ubuntu AAfD 32-bit and 64-bit (deb)	RedHat SUSE Linux AAfD 32-bit and 64-bit (rpm)	MacOS AAfD 64-bit (dmg)
Plantronics 300DA	Advanced	Basic	Basic	Basic	Voice
Plantronics 628 USB	Advanced	Voice	Voice	Voice	Advanced
Plantronics C510	Advanced	Voice	Voice	Voice	Advanced
Plantronics C310	Advanced	Voice	Voice	Voice	Advanced
Plantronics C520	Advanced	Voice	Voice	Voice	Advanced

Table continues…

Headset / Adaptor	Windows AAfD 32-bit (exe)	Windows AAfD 64-bit (exe)	ThinPro, Debian, Ubuntu AAfD 32-bit and 64-bit (deb)	RedHat SUSE Linux AAfD 32-bit and 64-bit (rpm)	MacOS AAfD 64-bit (dmg)
Plantronics C5200	Advanced	Voice	Voice	Voice	Advanced
Plantronics C3200	Advanced	Voice	Voice	Voice	Advanced
Plantronics DA 60	Voice	Voice	Voice	Voice	Voice
Plantronics DA 80	Advanced	Basic	Basic	Basic	Advanced
Plantronics SAVI 745 Wireless	Voice	Voice	Voice	Voice	Voice
Plantronics SAVI 420 Wireless	Voice	Voice	Voice	Voice	Voice
Plantronics DA55 / A / DA60 USB	Voice	Voice	Voice	Voice	Voice
Plantronics Blackwire 315.1 USB	Advanced	Basic	Basic	Basic	Voice
Plantronics Blackwire C220 M USB	Advanced	Basic	Basic	Basic	Voice
Plantronics Blackwire C610 USB	Advanced	Voice	Voice	Voice	Voice

Fully supported adapters:

- Plantronics DA80
- Plantronics DA90

Voice only supported adapter:

- Plantronics DA60

Note:

The mute button of Avaya Agent for Desktop instance in Desk Phone mode can now control and mute or unmute the microphone of Avaya Agent for Desktop in the local session in My Computer mode. This functionality is applicable for SIP mode only.

Interoperability

Table 5: Avaya Aura servers (for SIP)

Avaya Aura Server	Version
Avaya Aura® Communication Manager	7.1.x, 8.0.x, 8.1.x
Avaya Aura® System Manager	7.1.x, 8.0.x, 8.1.x
Avaya Aura® Session Manager	7.1.x, 8.0.x, 8.1.x
Avaya Aura® Session Border Controller	7.2.x, 8.0.x and 8.1.x
Avaya Aura® Application Enablement Services	7.1.x, 8.0.x, 8.1.x
Avaya WebLM Server	7.1.x, 8.0.x, 8.1.x
Avaya Contact Recorder	15.1, 15.2
Avaya Aura® Messaging server	7.1.x
Avaya Aura® Presence Services	8.0.x
Avaya Aura® Media Server	8.0.x, 8.1.x
Avaya Control Manager	8.1.0.1, 9.0.1
Avaya Call Management System	R 18.1, R19
Avaya Aura® Device Services	8.0.2.0.288

Table 6: Avaya Aura servers (for H.323)

Avaya Aura Server	Version
Avaya Aura® Communication Manager	7.1.x, 8.0.x, 8.1.x
Avaya Aura® System Manager	7.1.x, 8.0.x, 8.1.x
Avaya Aura® Application Enablement Services	8.0.x, 8.1.x
Avaya WebLM Server	8.0.x, 8.1.x
Avaya Contact Recorder	15.2
Avaya Aura® Messaging server	7.1.x
Avaya Aura® Media Server	8.0.x
Avaya Control Manager	8.1.0.1, 9.0.1
Avaya Call Management System	R 18.1, R19
Avaya Aura® Device Services	8.0.2.0.288

Table 7: Avaya Deskphone and Clients

Clients	Version
96x1	7.1.2.0.14
J179	3.0.0.0.20, 4.0.3.0.10

Table continues…

Avaya Workspaces for Elite	3.7.0.1
Avaya Oceana Workspaces	3.7.0.1

Table 8: Third-Party Platforms

Verified Platforms	Versions/Remarks
Windows 10	32 and 64 bits
MAC OS	10.14 and 10.15 only
HP T730	Debian Linux (ThinPro 6.x) 64 Bits
HP T630	WES 10 iOT
HP T530	WES 10 IOT, Debian Linux (ThinPro 6.x) 64 Bits
IGEL Universal Management Suite (UMS)	5
Ubuntu	18.0
HP T520	WES7

Table 9: Virtual Desktop Infrastructure

Verified Platforms	Versions
Citrix Xen App (32 Bits)	7.14.1
Citrix Xen Desktop (32 Bits)	7.14.1
VMware Horizon view	7.0

Avaya Oceana™ Workspaces supported scenarios

Scenarios with Avaya Oceana™ Workspaces	With SIP and H.323
Login/Logout Agent with Workspace	Yes
Incoming and outgoing call with Workspace	Yes
ACD Call with Ready mode	Yes
Hold/unhold	Yes
Direct Transfer	Yes
Consult Transfer	Yes
Conference	Yes
After Call Work (ACW)	Yes
My Computer Mode	Yes
Other Phone Mode	Yes

Note:

Due to H.323 limitation, Aux reason code is not syncing with Workspaces and Avaya Agent for Desktop.

Avaya Workspaces for Elite supported scenarios

Scenarios with Avaya Workspaces for Elite	With SIP and H.323
Login/Logout Agent with Workspace	Yes
Incoming and outgoing call with Workspace	Yes
ACD Call with Ready mode	Yes
Hold/unhold	Yes
Direct Transfer	Yes
Consult Transfer	Yes
Conference	Yes
After Call Work (ACW)	Yes
My Computer Mode	Yes
Other Phone Mode	Yes
Shared Control Mode	Yes

Note:

Due to H.323 limitation, Aux reason code is not syncing with Workspaces and Avaya Agent for Desktop.

Avaya Agent for Desktop usage scenarios

There are various methods of using the Avaya Agent for Desktop application, such as:

- Avaya Agent for Desktop VDI solution with H.323
- Avaya Agent for Desktop VDI solution with SIP
- Avaya Agent for Desktop standalone solution for H.323
- Avaya Agent for Desktop standalone solution for SIP
- Avaya Agent for Desktop remote agent solution for both VPN and SBC
- Avaya Agent for Desktop telecommuter mode with H.323
- Avaya Agent for Desktop telecommuter mode with SIP
- Avaya Agent for Desktop with shared control as controller with H.323
- Avaya Agent for Desktop with shared control as controller with SIP
- Avaya Agent for Desktop Headless Mode for H.323
- Avaya Agent for Desktop Headless Mode for SIP

Avaya Agent for Desktop VDI solution with H.323

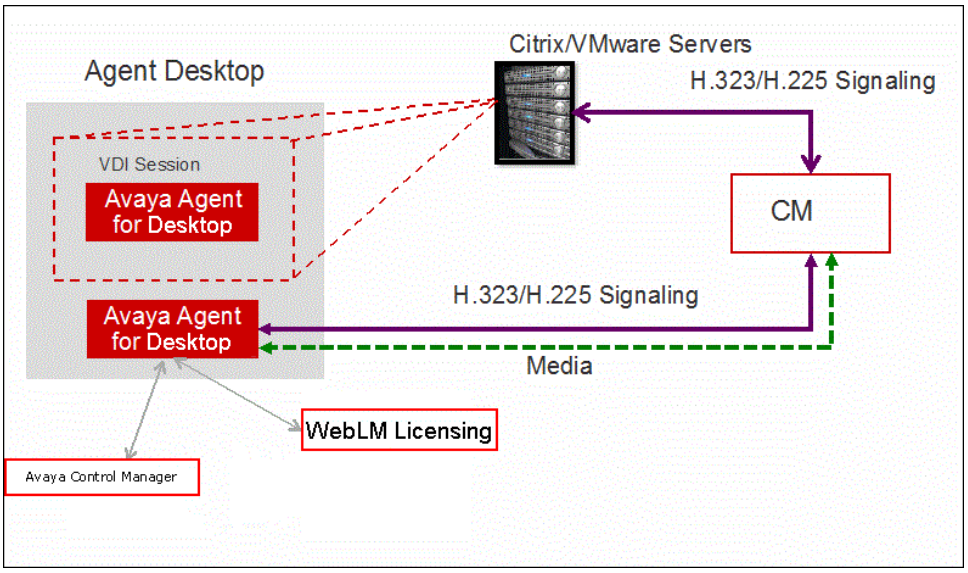


Figure 3: Avaya Agent for Desktop VDI solution with H.323

Avaya Agent for Desktop VDI solution with SIP

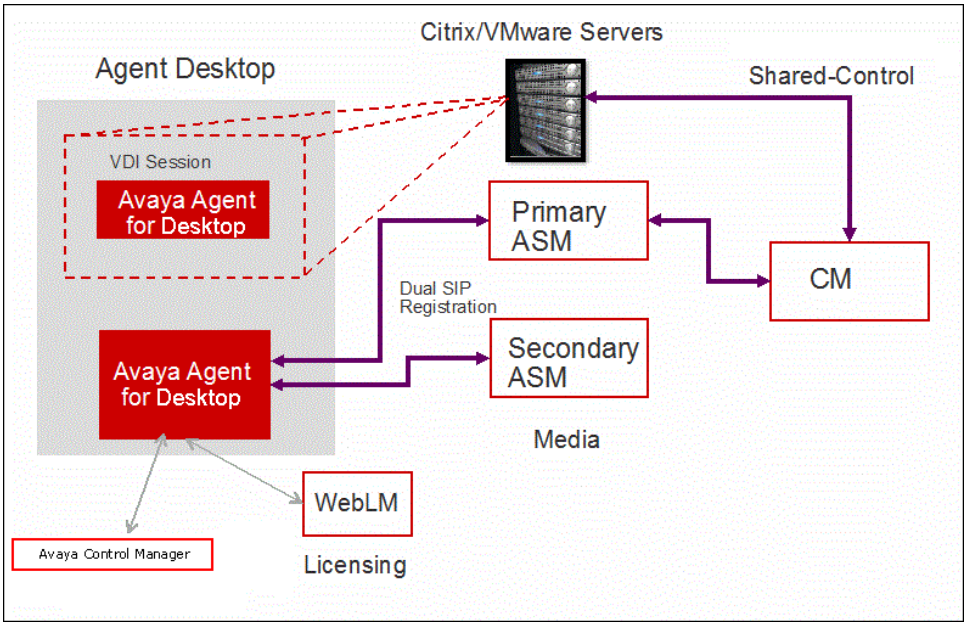


Figure 4: Avaya Agent for Desktop VDI solution with SIP

Avaya Agent for Desktop standalone solution for H.323

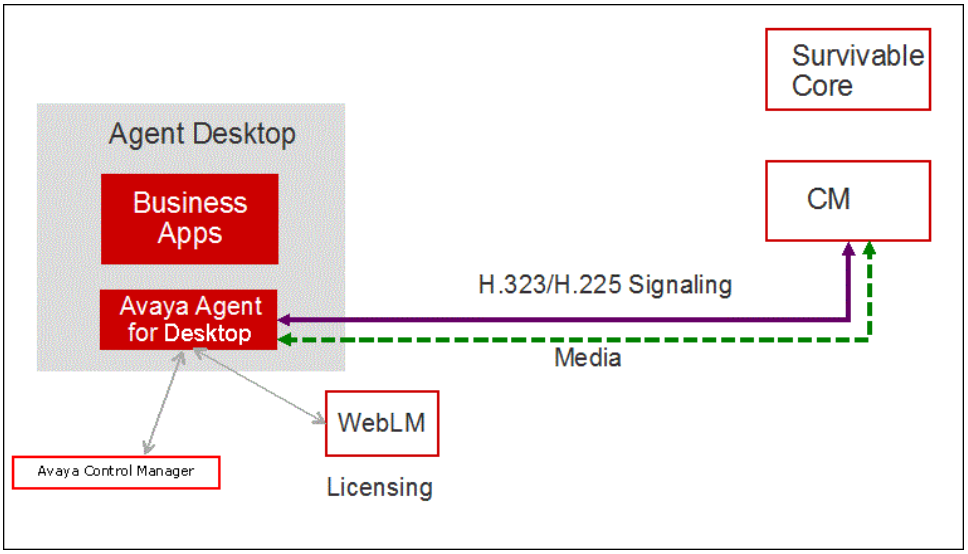


Figure 5: Avaya Agent for Desktop standalone solution for H.323

Avaya Agent for Desktop standalone solution for SIP

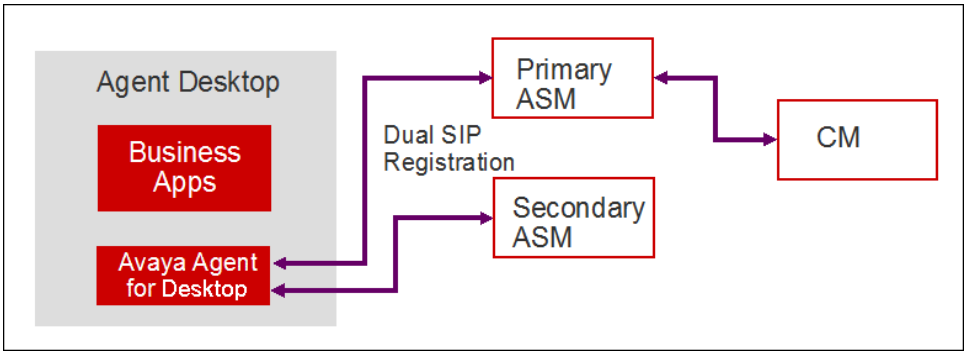


Figure 6: Avaya Agent for Desktop standalone solution for SIP

Avaya Agent for Desktop remote agent solution for both VPN and SBC

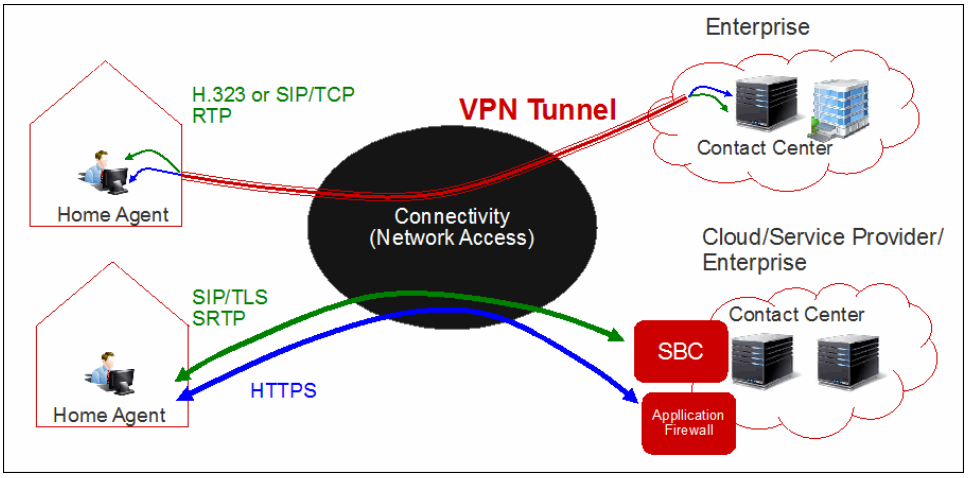


Figure 7: Avaya Agent for Desktop remote agent solution for both VPN and SBC

Avaya Agent for Desktop telecommuter mode with H.323

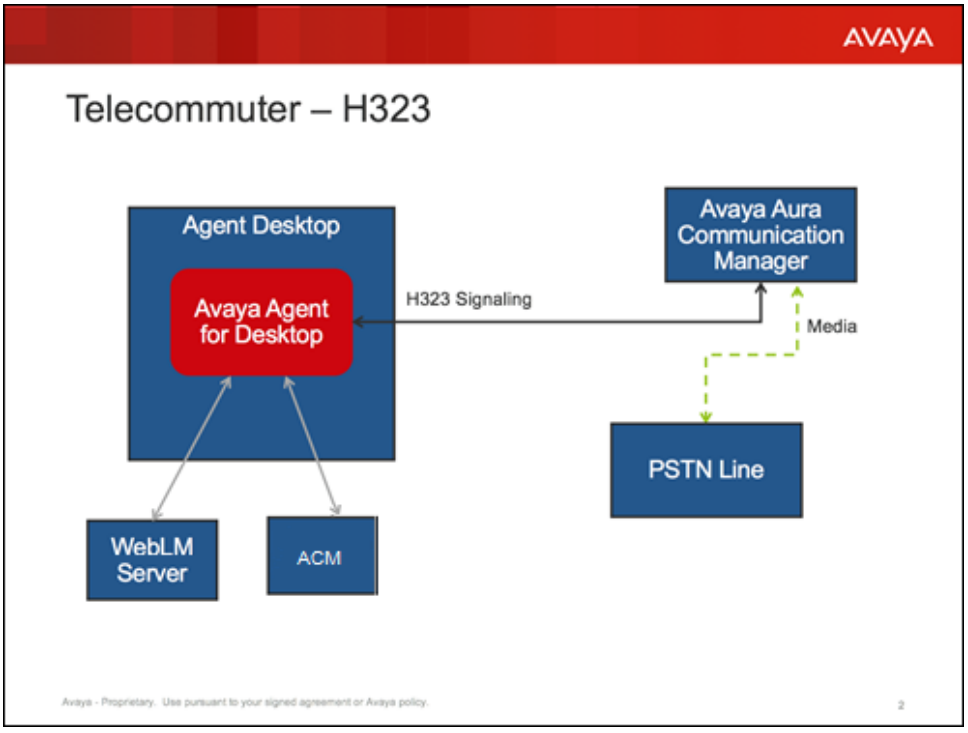


Figure 8: Avaya Agent for Desktop telecommuter mode with H.323

Avaya Agent for Desktop Telecommuter mode with SIP

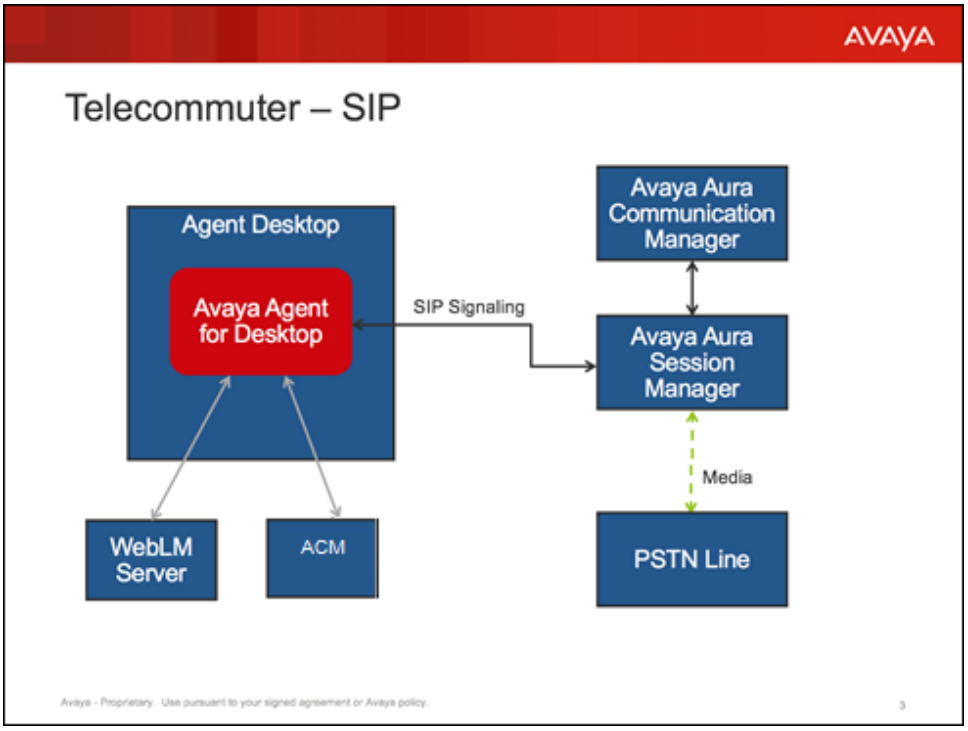


Figure 9: Avaya Agent for Desktop Telecommuter mode with SIP

Avaya Agent for Desktop with shared control as controller with H.323

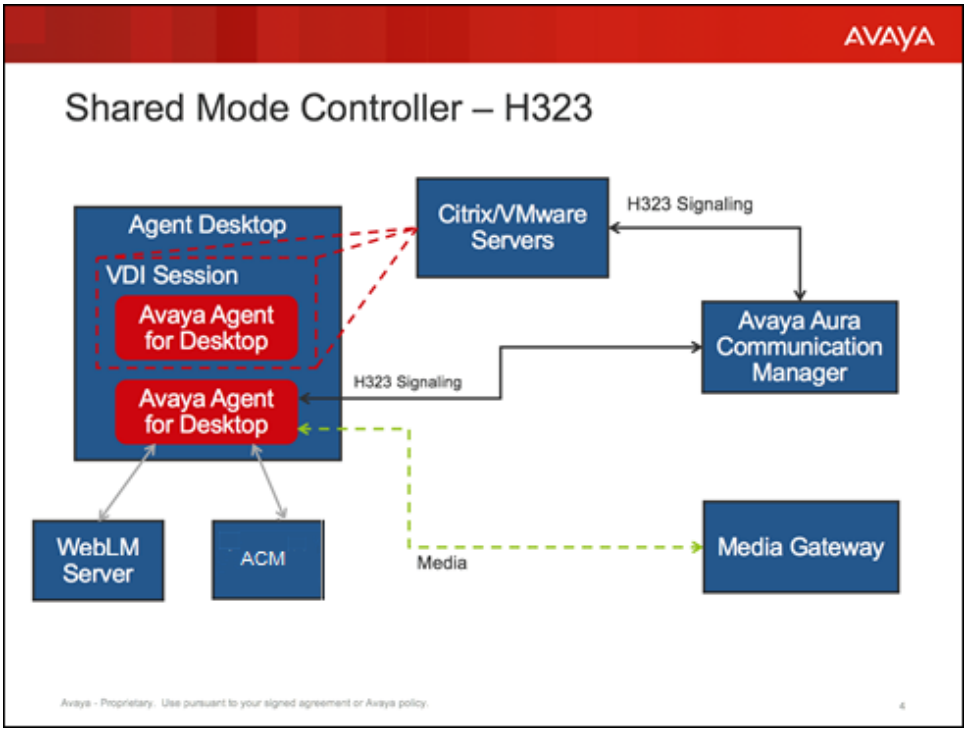


Figure 10: Avaya Agent for Desktop with shared control as controller with H.323

Avaya Agent for Desktop with shared control as controller with SIP

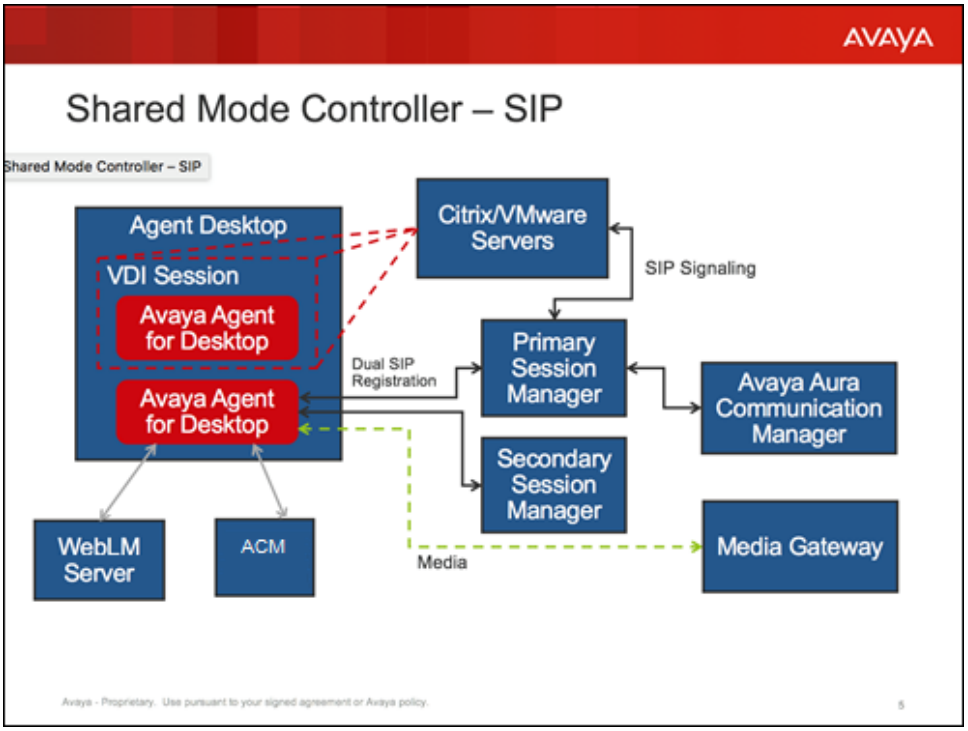


Figure 11: Avaya Agent for Desktop with shared control as controller with SIP

Avaya Agent for Desktop Headless Mode for H.323

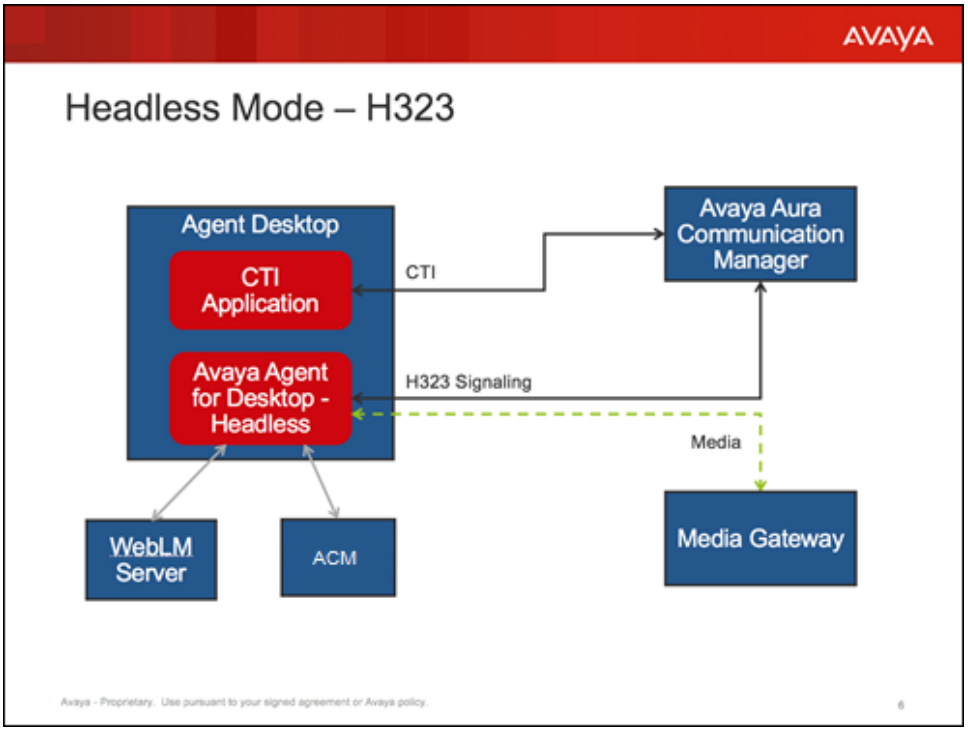


Figure 12: Avaya Agent for Desktop Headless Mode – H.323

Avaya Agent for Desktop Headless Mode for SIP

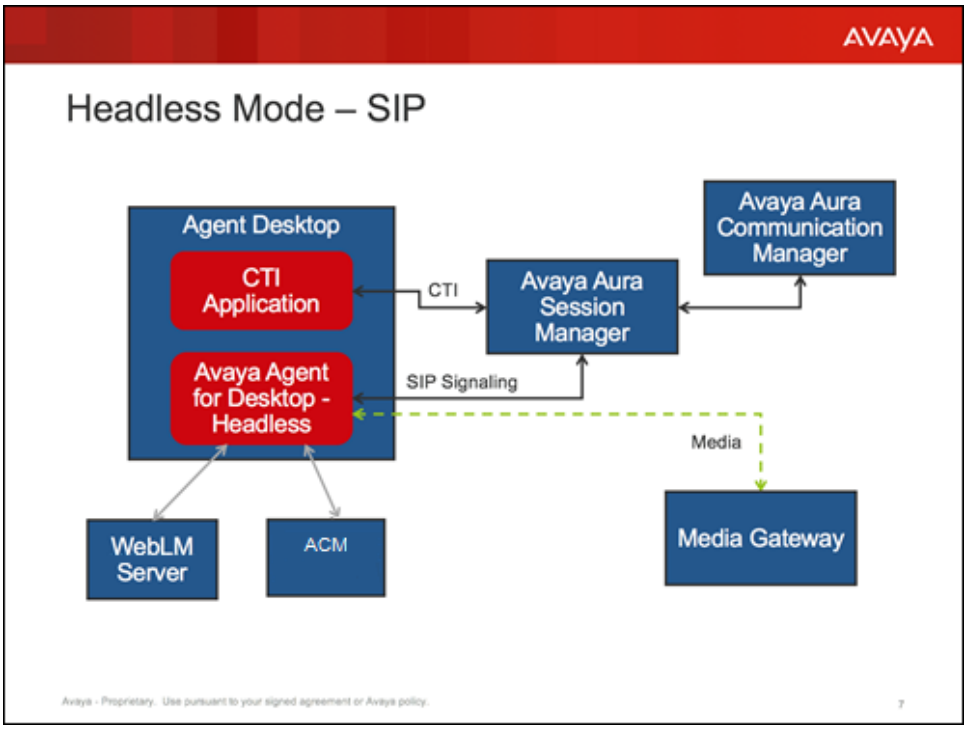


Figure 13: Avaya Agent for Desktop Headless Mode – SIP

Avaya Workspaces for Elite use case overview

You can use Avaya Agent for Desktop with Avaya Workspaces for Elite. In this case, you need to login only on station on the Avaya Agent for Desktop application, the call handling is handled through Avaya Workspaces for Elite through agent configured on Avaya Control Manager (ACM). The following diagram depicts how Avaya Agent for Desktop works with Avaya Workspaces for Elite:

Figure 14: Avaya Agent for Desktop with Avaya Workspaces for Elite

For more details on configuring Avaya Agent for Desktop on Avaya Workspaces for Elite , see the following sections of the *Deploying Avaya Workspaces for Elite* guide on the Avaya support portal:

- **Topology**
- **Creating an Avaya Workspaces agent user to handle Elite Voice contacts**
- **Creating an Avaya Workspaces supervisor user**

For more details on using Avaya Agent for Desktop on Avaya Workspaces for Elite, see the *Operations* section of the *Using Avaya Workspaces for Elite* guide on the Avaya support portal.

Chapter 3: Planning and preconfiguration

Installation checklist

Note:

While performing the Avaya Agent for Desktop upgrade, installation, or uninstallation tasks, ensure that you exit the Chrome browser, otherwise the plug-in for Chrome for click-to-dial browser extension does not work as expected.

The following checklist outlines the required installation steps for Avaya Agent for Desktop.

No.	Task	Notes	✔
1	Obtain the Avaya Agent for Desktop installation file.	The Avaya Agent for Desktop installer is available through Avaya Product Licensing and Delivery System (PLDS).	
2	Install an FTP server on the Data Center server.	The FTP server ensures the file transfer capabilities necessary for the Avaya Agent for Desktop for VDI deployment.	
3	Install an FTP client on the thin clients.	An FTP client must be configured on every thin client used for the Avaya Agent for Desktop for VDI deployment.	
4	Install Avaya Agent for Desktop.	You can install Avaya Agent for Desktop using one of the following methods: • Through the FTP server • Using the thin clients Device Manager	

Related links

Obtaining the Avaya Agent for Desktop installer on page 44

Obtaining the Avaya Agent for Desktop installer

To obtain the Avaya Agent for Desktop installer, you must use Avaya Product Licensing and Delivery System (PLDS) and select the version that is appropriate for your operating system.

The Avaya Agent for Desktop installer is available with the .exe extension for Windows systems, the .deb and .rpm extensions for Linux systems. The Mac version is delivered by the .dmg file.

Related links

Installation checklist on page 44
Downloading software from PLDS on page 45

Downloading software from PLDS

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. On the PLDS website, enter your Login ID and password.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Click the search icon ( ) for Company Name.
6. In the Search Companies dialog box, do the following:
   a. In the **%Name** field, type `Avaya` or the Partner company name.
   b. Click **Search Companies**.
   c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
   - In **Download Pub ID**, type the download pub ID.
   - In the **Application** field, click the application name.
8. Click **Search Downloads**.
9. Scroll down to the entry for the download file, and click the **Download** link.
10. Select a location where you want to save the file, and click **Save**.
11. **(Optional)** If you receive an error message, click the message, install Active X, and continue with the download.
12. **(Optional)** When the system displays the security warning, click **Install**.

    When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Related links

Obtaining the Avaya Agent for Desktop installer on page 44

Chapter 4: Installation and configuration

Installation modes

Following are the installation modes for Avaya Agent for Desktop:

Table 10:

Number	Installation mode	Reference
1.	Avaya Agent for VDI through FTP server	Installing Avaya Agent for Desktop on HP thin clients using an FTP server on page 49
2.	Avaya Agent for VDI remotely	Installing Avaya Agent for Desktop on t620 HP WES using HPDM on page 50 and Installing Avaya Agent for Desktop on HP ThinPro - 64 bits on page 52
3.	As a standalone Windows application	Installing Avaya Agent for Desktop as a standalone Windows application on page 54
4.	As a standalone Mac application	Installing Avaya Agent for Desktop as a standalone Mac application on page 56
5.	On Linux	Installing Avaya Agent for Desktop on Linux with RPM-based package on page 57 and Installing Avaya Agent for Desktop on Linux with DEB-based package on page 58
6.	Headless mode	Avaya Agent for Desktop for headless mode overview on page 58
7.	Silent installation on Windows	Performing silent installation of Avaya Agent for Desktop on Windows on page 61
8.	On the Lenovo M600 server	Installing or upgrading Avaya Agent for Desktop on the Lenovo M600 server on page 63
9.	On IGEL thin client using the IGEL UMS	Installing Avaya Agent for Desktop on IGEL thin client using the IGEL UMS on page 67

Table continues…

Number	Installation mode	Reference
10.	On IGEL client using UMS console	Installing Avaya Agent for Desktop on IGEL client using UMS console on page 68

Installing Avaya Agent for VDI through FTP server

Configuring the FTP server for a Linux thin client for VDI deployment

Before you begin

Create a folder structure for the FTP thin client.

You must place the configuration files and other necessary files in this folder structure as required by the installation process.

About this task

Perform the following steps to install the FTP server for a Linux thin client:

Procedure

1. Set up an FTP server in your environment.
2. Copy the Avaya Agent for Desktop .rpm file that is appropriate for your thin client to the `Wyse/add-ons` folder created on the FTP server.
3. Ensure that a `wlx` folder containing a `wlx.ini` file is placed in the same location as the `add-ons` folder. The contents of a typical `wlx.ini` file are the following:
   - `Update.Mode=Addons`
   - `Update.Preserve_changes=No`
   - `NewAddons=Avaya-Agent`
   - `RemoveAddons=Avaya-Agent`

Example

The following image provides an example structure for the FTP server directory:

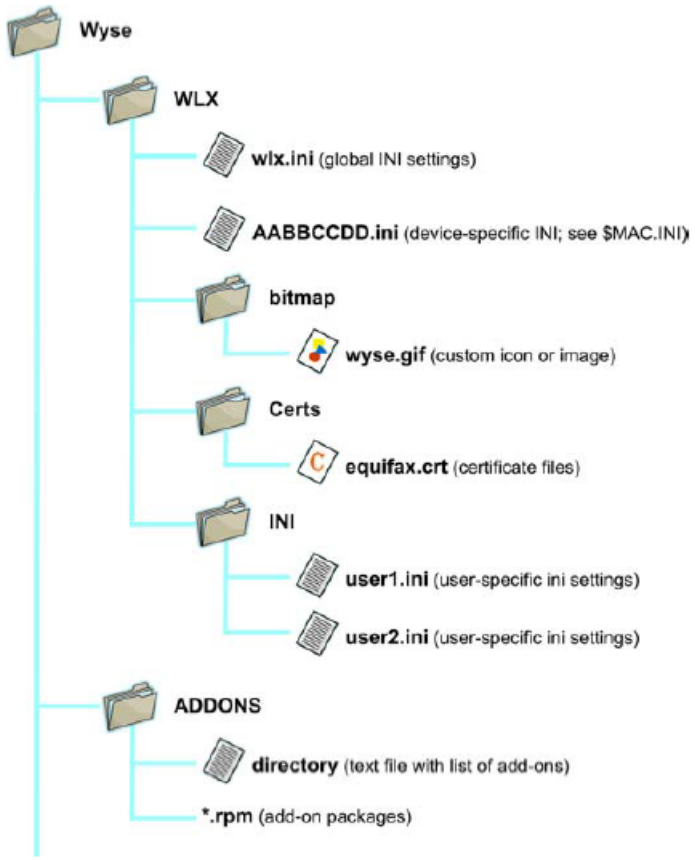


Figure 15: Wyse directory structure

Configuring the FTP server for a Windows thin client for VDI deployment

Before you begin

Create the following folder structure for the FTP server: `C:/inetpub/ftproot`.

You must place the configuration files and other necessary files in this folder structure as required by the installation process.

About this task

To configure the FTP server for a Windows thin client, perform the following actions:

Procedure

1. Set up an FTP server in your environment.
2. Create the `HP` folder under `C:/inetpub/ftproot`
3. Copy all the applications to the `C:/inetpub/ftproot/HP` folder.

Installing Avaya Agent for Desktop on HP thin clients using an FTP server

About this task

The following procedure describes the steps to install Avaya Agent for Desktop on an HP t520 Windows Embedded Standard (WES 7) OS-based HP thin client, using an FTP server.

Procedure

1. Start the HP thin client and log in as Administrator.
2. Perform the following actions to disable the write filter:
   a. Select **Start** > **HP Write Filter Configuration** .
   b. On the **General** tab, select the **Disable Write Filter** check box.
   c. Click **Apply**.
   d. Restart the thin client.
3. Start Internet Explorer and enter the IP address of the FTP server in the address bar.
4. Double-click the Avaya Agent for Desktop executable file.
5. Click **Run** in the **Open File** dialog box.
6. In the Avaya Agent for Desktop Setup window, perform the following actions:
   a. Click **Next**.
   b. On the License Agreement page, click **I Agree**.
   c. Click the **Browse** button to choose an installation directory.

      The default installation directory is `C:\Program Files\Avaya\Avaya Agent`.
   d. Click **Next**.
   e. Select a start menu folder for Avaya Agent for Desktop.
   f. Click **Install**.
   g. Click **Finish** when the installation is complete.

Next steps

After the installation is complete, right-click on the padlock on the bottom right of the screen and select **Enable FBWF(E)**.

The **Enable EBWF(E)** option enables the write filter, making the file system read only.

Uninstalling Avaya Agent for Desktop from HP clients

Before you begin

Stop Avaya Agent for Desktop.

Procedure

1. Navigate to the Avaya Agent for Desktop folder.
2. Click Uninstall.exe.
3. In the Avaya Agent for Desktop Uninstall wizard, click **Uninstall**.

   The system displays a message to confirm that the uninstall process is complete.
4. Click **Close** to close the wizard.

Installing Avaya Agent for VDI remotely

Installing Avaya Agent for Desktop on t620 HP WES using HPDM

Before you begin

Before you install Avaya Agent for Desktop, ensure that an FTP Server is installed on the station.

About this task

The following procedure describes the steps to install Avaya Agent for Desktop on an HP t620 Windows Embedded Standard (WES 7) OS-based HP thin client, using HP Device Manager (HPDM).

Procedure

1. Install HPDM Server.

   Note:

   During the installation, open the `C:/inetpub/ftproot` folder and create the following folder structure: `C:/inetpub/ftproot/HPDM/server/Repository/Files/Push to Agent`
2. Download the Avaya Agent for Desktop installer to the HPDM server and copy the installer to `C: /inetpub/ftproot/HPDM/server/Repository/Files/Push to Agent`.
3. Run the HPDM console.
4. In the **HP WES/XPe** tab, select **File and Registry**.
5. Right-click on the *File And Registry* template and select **Properties**.
6. In the Template Editor – File and Registry window, create a copying task for the Avaya Agent for Desktop installer:
   a. In the **Content** tab, click **Add** and select **Copy Files**.

      The system displays the Copy Files Sub-Task window.

b. In the **FTP Repository** field, select **Use Default FTP** and in the **Direction** field, select **Download**.

c. In the Files to be copied section, set the **File or Folder Name** to the name of the Avaya Agent installer file, and set the **Path On Device** to `C:\TEMP`.

d. Click **OK**.

The system creates a copying task for the Avaya Agent installer to the `C:\TEMP` folder on the devices.

7. In the Content tab, perform the following actions:

a. select **Add** > **Command** and enter the following installation commands:

```
ewfmgr -all -disable
C:\TEMP\avaya-agent-0.0.0.1130-win.exe /S /ACCEPTEULA=yes
fbwfmgr /enable
C:\Program Files\Avaya\Avaya Agent\bin\wes7\avaya-agent-add-wf-exclusion.bat
```

b. In the **Wait** field, select **Yes** for all the commands.

c. Click **OK**.

8. Click the **Save As** button to save the template.
9. Right-click the template and select **Send Task**
10. In the Task Editor window, click **Add** to specify the necessary devices and click **OK** to send the task.

Next steps

Once the task completes, navigate to the next tabs to see your computers. The HP WES/XP machines are the Windows machines.

To update an Agent, right-click the machine to update and select **Send Task**.

For more information about how to install add-ons on HP thin clients using HPDM, see the *HP Device Manager User Guide* available on the HP Web site.

Uninstalling Avaya Agent for Desktop from t620 HP WES using HPDM

Procedure

1. Start the HPDM console.
2. In the **HP WES/XPe** tab, select **File and Registry**.
3. Right-click the `_File And Registry` template and select **Properties**.
4. In the content tab, select **Add** > **Command** and add the following command:

```
C:\Program Files\Avaya\Avaya Agent\Uninstall.exe /S
```

5. Click **Save As** to save the new task as a template.

6. Right-click the template and select **Send Task** to use it for all the managed HP Thin Pro-based clients.

Installing Avaya Agent for Desktop on HP ThinPro - 64 bits

Before you begin

Before you install Avaya Agent for Desktop, ensure that an FTP Server is installed on the station.

About this task

Use this procedure to install Avaya Agent for Desktop on HP ThinPro - 64 bits.

Procedure

1. Install the HPDM server.

   Note:

   During the installation, open the `C:/inetpub/ftproot` folder and create the following folder structure: `C:/inetpub/ftproot/HPDM/server/Repository/Files/Push to Agent`.

2. Download the Avaya Agent for Desktop installer to the HPDM server and copy the installer to `C:/inetpub/ftproot/HPDM/server/Repository/Files/Push to Agent`.
3. Run the HPDM console.
4. In the **Discover Device** dialog box, perform the following actions:
   a. **Select HPDM Gateway**.
   b. **Select Device type**.
   c. Click **Walk With IP Range**.
5. Click **Next**.
6. On the **HP ThinPro 5** tab, right-click the appropriate thin client and click **Send Task**.
7. In the **Template Chooser** dialog box, in **Category**, click **File and Registry**.
8. In **Template**, click **File and Registry** and click **Next**.
9. In the **Task Editor** dialog box, click **Add**.
10. In the **Sub-Task Chooser** dialog box, click **Deploy Files** and click **OK**.
11. In the **Deploy Files** dialog box, perform the following actions:
    a. Click **Add from Local**.
    b. Locate and select the Avaya Agent for Desktop thin pro installer from the `Push to Agent` folder.
    c. In the **Path on Device** field, enter `/tmp`.
12. Click **OK**.

13. In the **Task Editor** dialog box, click **Add**.
14. In the **Sub-Task Chooser** dialog box, click **Command** and click **OK**.
15. In the **Execute Command Sub-Task** dialog box, perform the following actions:
    a. In the **Command** field, enter the following commands:

    ```
    fsunlock
    dpkg -i /tmp/avaya-agent-2.0.0.xxx_amd64.deb
    rm /tmp/avaya-agent-2.0.0.xxx_amd64.deb
    fslock
    ```

    b. In the **Wait** field, select **Yes** for all commands.
16. Click **OK**.
17. Click the **Save As** button to save the task as a template and use the task to deploy Avaya Agent for Desktop to all managed HP ThinPro-based bricks.
18. Right-click the template, and select **Send Task**.
19. In the **Task Editor** dialog box, click **Add** and specify the necessary devices.
20. Click **OK** to send the task.

Next steps

You can verify the status of the tasks on the **Manual Tasks** tab at the bottom of the console.

For more information about how to install add-ons on HP thin clients using HPDM, see the *HP Device Manager User Guide 4.6* available on an HP website.

Uninstalling Avaya Agent for Desktop from HP ThinPro-64 bits

Procedure

1. Start the HPDM console.
2. On the **HP ThinPro** tab, right-click the appropriate thin client and click **Send Task**.
3. In the **Template Chooser** dialog box, in **Category**, click **File and Registry**.
4. In **Template**, click **File and Registry** > **Next**.
5. In the **Task Editor** dialog box, click **Add**.
6. In the **Sub-Task Chooser** dialog box, click **Command** and click **OK**.
7. In the **Execute Command Sub-Task** dialog box, in the **Command** field, enter the following commands:

    ```
    fsunlock
    dpkg -r avaya-agent
    fslock
    ```

8. Click **OK**.
9. Click the **Save As** button to save the new task as a template.

Installing Avaya Agent for Desktop as a standalone Windows application

Installing Avaya Agent for Desktop as a standalone Windows application

Procedure

1. Download the latest Avaya Agent for Desktop installer file from Avaya PLDS.
2. Right-click the installer file (.exe) saved at the download location and click **Run as Administrator**.

   The system displays the Select Setup Language dialog box.
3. Select the language as configured for your operating system and click **OK**.

   The system displays the Setup – Avaya Agent installation wizard.
4. Click **Next** .

   The system displays the Destination screen.
5. Specify the installation destination and click **Next** .

   The system displays the Select Start Menu Folder screen.
6. Specify the folder name and click **Next** .

   The system displays the click to dial Browser Extension screen.
7. Select the browser/s for which you want to install the click to dial browser extensions and click **Next**.

   The system displays the Additional Tasks screen.
8. Select the required options and click **Next**.

   The system displays the Ready to Install screen.
9. Click **Install**.

   The Avaya Agent for Desktop is installed on your system and confirmation screen is displayed.
10. Ensure that the **Launch Avaya Agent** check box is selected and click **Finish**.

    The system displays the End User License Agreement window.
11. Click **Install**.

    The Avaya Agent for Desktop is installed on your system and confirmation screen is displayed.
12. Ensure that the **Launch Avaya Agent** check box is selected and click **Finish**.

The system displays the Avaya Agent for Desktop Welcome window.

13. From the **Select the language** drop-down list, select a language that you want set as the default UI language of the application.
14. Click **Next**.

    The system displays the End User License Agreement (EULA) screen in the selected UI langauge.
15. Read the agreement carefully and select **I Agree** to accept the Avaya Agent for Desktop EULA.
16. Click **Next**.

    The system displays the License Type screen.
17. In the **WebLM License Server Address** field, specify the WebLM license server address and click **Check**.

    If the license server address is valid and there are available licenses, then a check mark will appear next to the applicable license type options listed below the address field.
18. Select the applicable license type from the given options and click **Next**.

    Note:

    If WebLM server is unavailable or WebLM address was not entered properly, you can enter the same in the **Settings** configuration later. Avaya Agent for Desktop would still work in 30 days trial mode with functionality of the chosen license type. Also, the system will display or hide UI and other configuration options of the application based on the license type selected.

    The system displays the Ready screen.
19. Click **Launch**.

    The system installs the Avaya Agent for Desktop application on your system.

Uninstalling Avaya Agent for Desktop standalone application from Windows machine

Procedure

1. Go to **Start** > **Control Panel**.
2. Click **Programs and Features**.

   The system displays the Programs and Features window.
3. From the list of installed application, click Avaya Agent for Desktop.
4. Click **Uninstall/Change**.

   The system displays the Avaya Agent Uninstall window.

5. Click **Uninstall**.
6. Click **Close** to complete the uninstallation process.

Installing Avaya Agent for Desktop as a standalone Mac application

Installing Avaya Agent for Desktop as a standalone Mac application

Procedure

1. Download the latest Avaya Agent for Desktop installer file for Mac from Avaya PLDS.
2. Double-click the installer file (Darwin, .dmg) saved at the download location.

   The system mounts the .dmg file which contains the Avaya Agent for Desktop application.
3. Open the mounted image of Avaya Agent for Desktop.
4. Drag and drop the Avaya Agent for Desktop application file in the **Applications** folder. or double-click the application file.

   The system displays the Avaya Agent for Desktop Welcome window.
5. From the **Select the language** drop-down list, select a language that you want set as the default UI language of the application.
6. Click **Next**.

   The system displays the End User License Agreement (EULA) screen in the selected UI langauge.
7. Read the agreement carefully and select **I Agree** to accept the Avaya Agent for Desktop EULA.
8. Click **Next**.

   The system displays the License Type screen.
9. In the **WebLM License Server Address** field, specify the WebLM license server address and click **Check**.

   If the license server address is valid and there are available licenses, then a check mark will appear next to the applicable license type options listed below the address field.
10. Select the applicable license type from the given options and click **Next**.

Note:

If WebLM server is unavailable or WebLM address was not entered properly, you can enter the same in the **Settings** configuration later. Avaya Agent for Desktop would still work in 30 days trial mode with functionality of the chosen license type. Also, the system will display or hide UI and other configuration options of the application based on the license type selected.

The system displays the Browser extension screen.

11. Click **Install** for the Google Chrome browser extension.
12. Click **Next**.

    The system displays the Ready screen.
13. Click **Launch**.

    The Avaya Agent for Desktop installation procedure is completed and the application is launched on your system for further configuration.

Uninstalling Avaya Agent for Desktop as a standalone application from a Mac machine

Procedure

1. Open the **Applications** folder located at `~/Library/Preferences/avaya-agent`.
2. Drag and drop the Avaya Agent for Desktop application icon to **Trash**.

   The system uninstalls Avaya Agent for Desktop from a Mac machine.

Installing Avaya Agent for Desktop on Linux

Installing Avaya Agent for Desktop on Linux with RPM-based package

Before you begin

Uninstall the earlier version of Avaya Agent for Desktop.

Ensure that you have the latest version of Avaya Agent for Desktop RPM package.

Procedure

1. Copy the Avaya Agent for Desktop RPM package to your work folder.
2. Run the following command:

```
sudo rpm -i --nodeps --force <Package_name.rpm>
```

Uninstalling Avaya Agent for Desktop on Linux with RPM-based package

Procedure

1. Run the command: **sudo rpm -e avaya-agent;**
2. If "`sudo rpm -e`" gets the error `specifies multiple packages`, then run: **sudo rpm -e --allmatches avaya-agent;**

Installing Avaya Agent for Desktop on Linux with DEB-based package

Before you begin

Uninstall the earlier version of Avaya Agent for Desktop.

Ensure that you have the latest version of Avaya Agent for Desktop DEB package.

Procedure

1. Copy the Avaya Agent for Desktop DEB package to your work folder.
2. Run the command: **sudo dpkg -i <Package_name.deb>**

Uninstalling Avaya Agent for Desktop on Linux with DEB-based package

Procedure

Run the command: **sudo dpkg -r avaya-agent**

Installing Avaya Agent for Desktop for a headless mode

Avaya Agent for Desktop for headless mode overview

In a headless mode, you can use the Avaya Agent for Desktop application without user interface. For controlling features of the application, you must use a CTI application or another client application. There is no separate installer for the headless mode anymore. The mode can be

chosen through the first launch of the application installation wizard by selecting the appropriate license type.

Checklist for configuring Avaya Agent for Desktop for a headless mode

Settings window

Note:

Refer to the **Settings** window field descriptions sections in this guide for configuring the Avaya Agent for Desktop for a headless mode.

Tab	Status	Description
Server	Enabled	All fields are enabled for this tab. You must configure the settings as per your requirement.
Dialing Rules	Disabled	All fields are disabled for this tab.
Preferences	Enabled	All fields are disabled for this tab.
Reason Codes	Disabled	All fields are disabled for this tab.
Audio	Enabled	All fields are enabled for this tab. You must configure the settings as per your requirement.
Greetings	Disabled	All fields are disabled for this tab.
Screen Pop	Disabled	All fields are disabled for this tab.
Advanced	Enabled	All fields are enabled for this tab. You must configure the settings as per your requirement.

License modes

The license mode defines which Avaya Agent for Desktop features are available for a particular license type. Refer the following table for more details:

License types/ Features	Advanced/ Standalone	Basic / (Shared Controlled with Avaya one-X® Agent)	Locked Down/ Headless	Deskphone
WebLM Feature Name	• VALUE_VDIA_ADVANCED_COUNTS • VALUE_VDIA_CONTROL_COUNTS	VALUE_VDIA_BASIC_COUNTS	VALUE_VDIA_HEADLESS_ONLY_COUNTS	This mode does not require WebLM feature. Here, a user is not limited to select deskphone login. But if a user select other login type, such as my computer, telecommuter, etc, then WebLM is used as per the Advanced/ Standalone license mode type.
Full UI	Yes	Yes	N/A	Yes
Headless UI	N/A	N/A	Yes	N/A
Collapsed UI Media Controls	Yes	Yes	N/A	Yes
H.323 Roadwarrior	Yes	Yes	Yes	Yes
SIP Roadwarrior	Yes	Yes	Yes	Yes
Desk Phone Mode	Yes	N/A	N/A	Yes
Other Phone/ Telecommuter	Yes	N/A	N/A	Yes
Media Quality Indicator	Yes	Yes	N/A	Yes
Dual Registration/ Failover	Yes	Yes	Yes	Yes
Stats Console	Yes	N/A	N/A	Yes
Screen Pop	Yes	N/A	N/A	Yes
VoIP Quality Monitoring	Yes	Yes	Yes	Yes
Supervisor Features	Yes	N/A	N/A	Yes
CTI Controlled	Yes	Yes	Yes	Yes x
Click to Call	Yes	Yes	Yes	Yes

Table continues…

License types/ Features	Advanced/ Standalone	Basic / (Shared Controlled with Avaya one-X® Agent)	Locked Down/ Headless	Deskphone
Headset Integration	Yes (for my computer mode only)	Yes	Yes	Yes (for my computer mode only)
Presence	Yes	Yes	N/A	Yes
Comments	If a user selects deskphone, then Avaya Agent for Desktop does not need to occupy the license.	-	-	It works mostly like an Advanced/ Standalone mode.

Other capabilities

- Log in on the extension using the Login dialog box.
- Use the CTI application or another client to sign in an agent.
- Login with ACM account is also supported.
- Use the CTI application for the management of calls and agent states.
- Notification with the current login status can be viewed with mouse-hover or by double-clicking the Avaya Agent for Desktop task bar icon.

  Note:

  Agent number is displayed only for SIP signaling.
- Right-click and click **Mute** in the task bar icon context menu to mute the microphone.

  Note:

  Mute action is available only when Avaya Agent for Desktop is registered.

Performing silent installation of Avaya Agent for Desktop on Windows

Procedure

1. To perform the silent installation with UI, navigate to `<Location of AAfD installer file>` and run the following command:

   ```
   avayaagent-x.y.z.aa.build-platform.exe /SILENT
   ```

   The system displays AAfD UI for silent installation.
2. To perform the silent installation without the UI, navigate to `<Location of AAfD installer file>` and run the following command:

```
avaya-agent-x.y.z.aa.build-platform.exe /VERYSILENT
```

The system runs silent installation in the background and does not display the UI for installation.

3. To perform the silent installation without UI and to set the log path, navigate to `<Location of AAfD installer file>` and run the following command:

   ```
   avaya-agent-x.y.z.aa.buildplatform.exe /verysilent /
   LOG="<InstallationLogPath>"
   ```

   The system runs silent installation in the background and sets the defined log path.

   `avaya-agent-x.y.z.aa.buildplatform.exe /silent /`
   `LOG="<InstallationLogPath>"`

   The system runs silent installation in the background with the UI and sets the defined log path.

4. To perform the silent installation without using a browser extension, navigate to `<Location of AAfD installer file>` and run the following command:

   ```
   avaya-agent-x.y.z.aa.build-platform.exe /VERYSILENT /NOEXTENSIONS
   ```

   The system runs silent installation in the background without using a browser.

   `avaya-agent-x.y.z.aa.build-platform.exe /SILENT /NOEXTENSIONS`

   The system runs silent installation with the UI in the background, without using a browser.

5. To perform the silent installation with browser extensions, navigate to `<Location of AAfD installer file>` and run the following command:

   Note:

   Close your Google Chrome browser before the installation starts.

   ```
   avaya-agent-x.y.z.aa.build-platform.exe /VERYSILENT /
   INSTALLEXTENSIONS
   ```

   The system runs silent installation in the background and installs browser extensions as well.

   `avaya-agent-x.y.z.aa.build-platform.exe /SILENT /INSTALLEXTENSIONS`

   The system runs silent installation in the background and installs browser extensions as well.

Installing or upgrading Avaya Agent for Desktop on the Lenovo M600 server

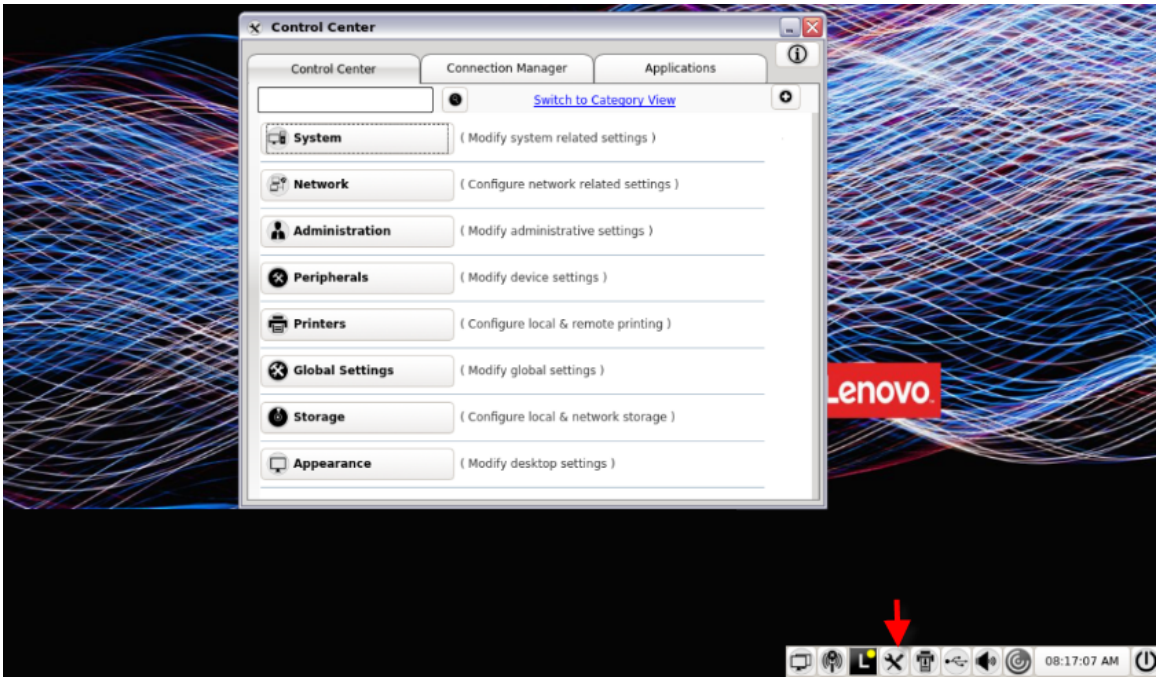
Before you begin

- Ensure that you have provided the latest installer file to Lenovo's customer support team.
- Ensure that you have received the .tar file of the latest installer shared with Lenovo's customer support team.
- Ensure that you have copied the latest .tar file on the Lenovo M600 server.

Procedure

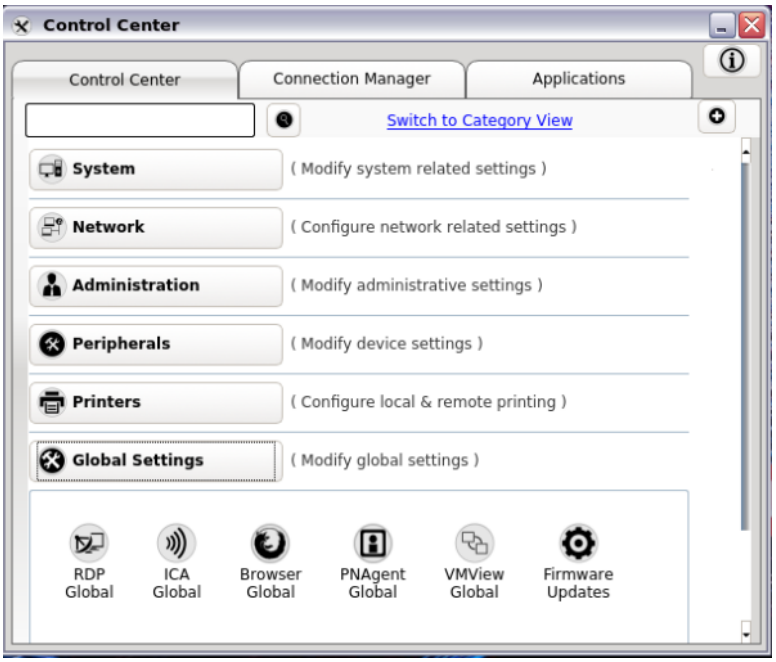
1. On Lenovo M600 server task bar, click **Control Center**.

   The system displays the Control Center settings window.



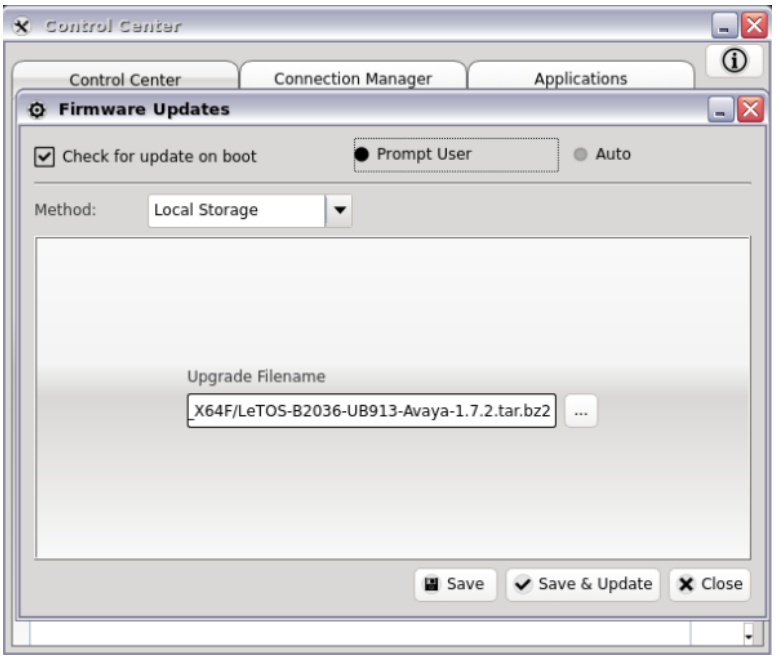
2. Click **Global Settings**.

   The system displays the Global Settings options.



3. Click **Firmware Updates (LetOS)**.

   The system displays the firmware update dialog box.



4. Select the **Check for update on boot** check box.
5. (Optional) Click **Mount** (if available).
6. In the **Method** drop down list, select **Local Storage**.
7. In **Upgrade File name**, click **Browse file**.

8. Select the .tar file stored on the Lenovo M600 server and click **Save & Update**.

   The installation process is completed and the Lenovo M600 server is restarted.

   Important:

   If you want to uninstall Avaya Agent for Desktop from the Lenovo M600 server, you need to contact Lenovo's customer support team administrator.

Next steps

Access the Avaya Agent for Desktop application on the Lenovo M600 server.

Accessing Avaya Agent for Desktop on the Lenovo M600 server

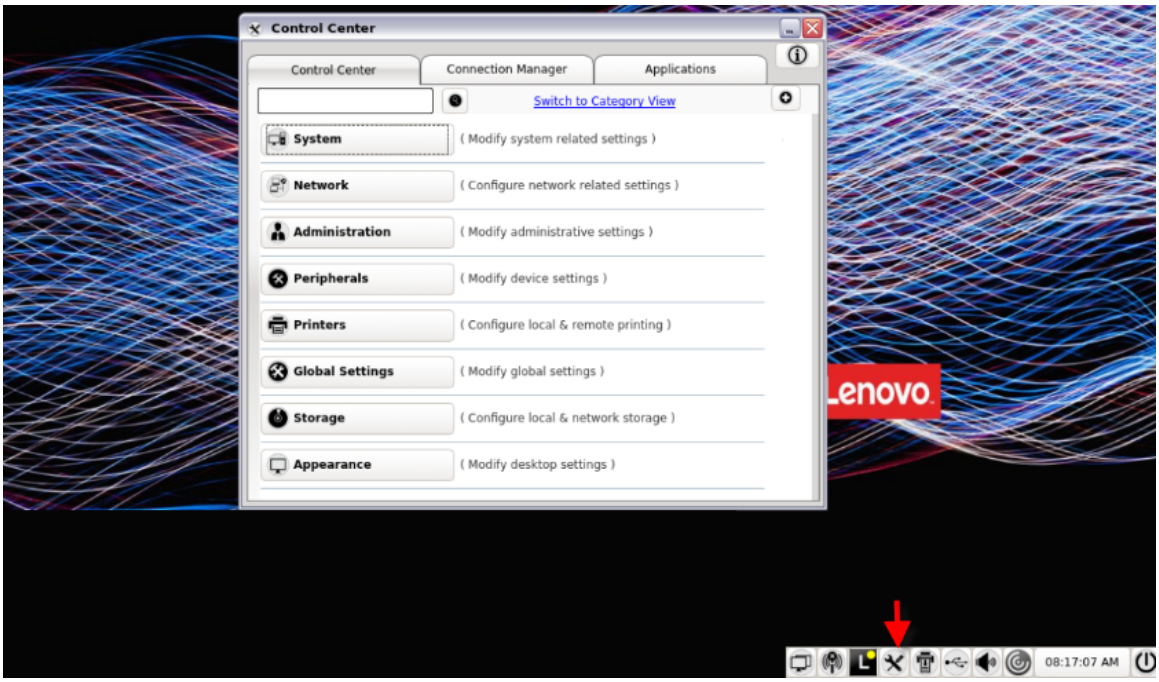
About this task

Use the following procedure to verify that Avaya Agent for Desktop is successfully installed on your Lenovo M600 server.

Procedure

1. On Lenovo M600 server task bar, click **Control Center**.

   The system displays the Control Center settings window.

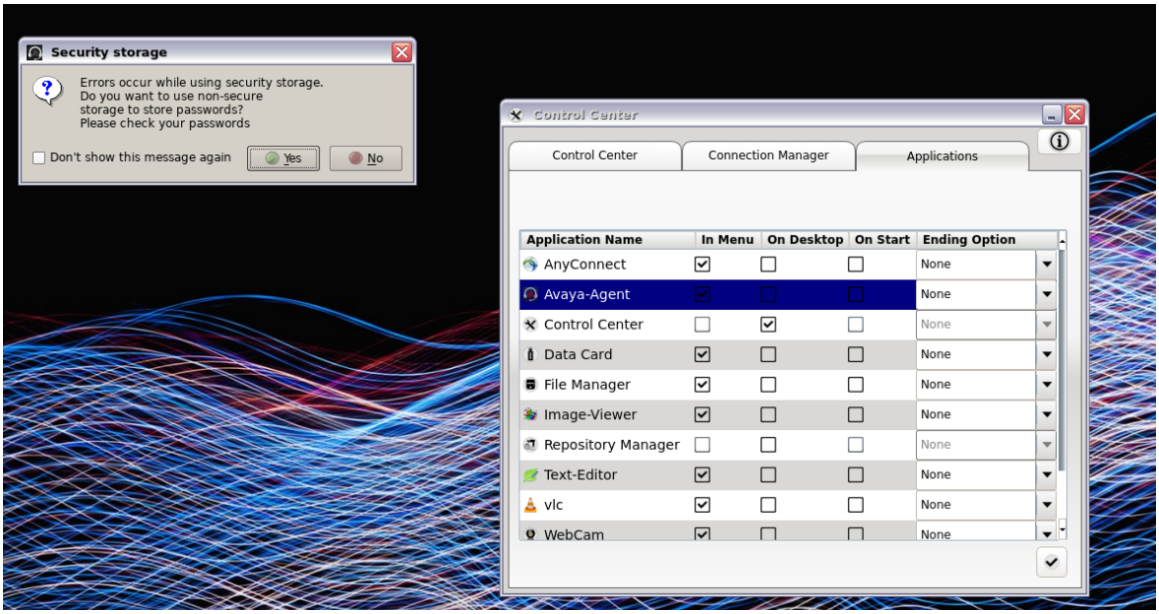


2. Click the **Applications** tab.

The system displays the Applications tab options.

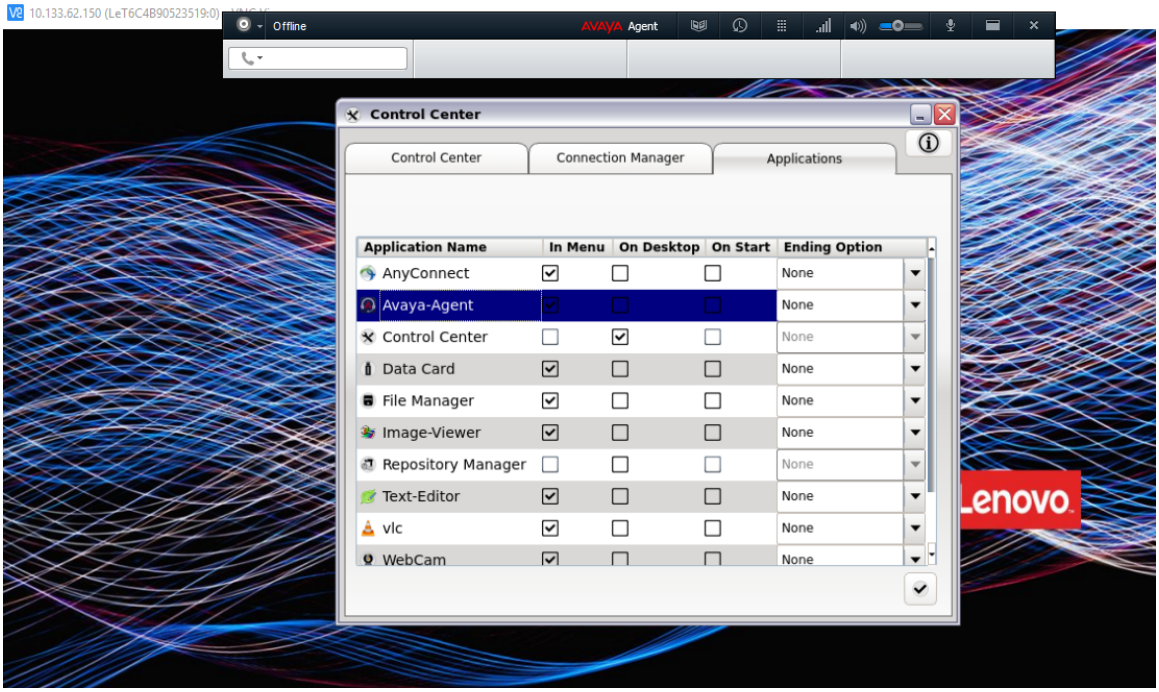
3. Scroll down and select the Avaya Agent for Desktop application option.

   The system displays the Certificate confirmation dialog box.



4. Click **Yes**.

   The system displays the Avaya Control Manager (ACM) login window in case of the ACM login mode else the system launches the Avaya Agent for Application on the server.



Overview of Avaya Agent for Desktop on IGEL thin client using the IGEL UMS

IGEL OS is a modular, read-only computer operating system. It is centrally managed by using the IGEL Universal Management Suite (UMS).

With the IGEL OS, Avaya Agent for Desktop (AAfD) is installed as a package called as Custom Partition. Custom Partition is deployed from a central repository by using the IGEL UMS.

Avaya Agent for Desktop installations on Linux thin clients are installed by using package management tools developed by Red Hat (.rpm) or Debian (.deb). With IGEL, Avaya Agent for Desktop is deployed by using a traditional tarball that is expanded and processed locally on the endpoint. The IGEL method is a controlled process that is initiated from UMS Console.

Installing Avaya Agent for Desktop on IGEL thin client using the IGEL UMS

Before you begin

Record the user name and password typed in for the database connection. You can do this by going under **User Credentials for DB-connect** during installation of the Universal Management Suite (UMS).

About this task

Use this procedure to install Avaya Agent for Desktop on IGEL thin client using the IGEL UMS.

Procedure

1. Ensure that the IGEL UMS must be set up and running on a computer.

   Note:

   During the UMS installation, navigate to **User Credentials for DB-connect** and record the following:

   - <ums_server> - the IP address or FQDN of the UMS Server
   - <ums-username> - the username typed in during installation
   - <ums-password> - the password typed in during installation

2. Set up the IGEL client and register to the UMS console.
3. Download the Avaya Agent for Desktop Custom Partition ZIP file from `support.avaya.com`.

   IGEL custom partitions are delivered as a ZIP archive. Each archive contains the following:

   - -igel : a folder that contains UMS profiles
   - -target : a folder that contains Custom Partition (inf and tar.bz2 files)

- -disclaimer.txt : a disclaimer note
- -readme.txt: a short installation guide

4. Unzip the Custom Partition archive.

Installing Avaya Agent for Desktop on IGEL client using UMS console

About this task

Use this procedure to install Avaya Agent for Desktop on IGEL client using UMS Console

Procedure

1. Copy the contents of the target folder to the ums_filetransfer folder on the UMS Server.

   Copy the files to the following file paths:

   On Windows, use :

   ```
   C:\Program Files (x86)\IGEL\RemoteManager\rmguiserver\webapps
   \ums_filetransfer\
   ```

   On Linux, use:

   ```
   /opt/IGEL/RemoteManager/rmguiserver/webapps/ums_filetransfer/
   ```

2. To confirm the accessibility of the Custom Partition files, type the following URL on a browser: `https://<ums_server>:8443/ums_filetransfer/avaya-agent.inf`, where <ums_server> is the FQDN or IP Address of the UMS server.

   ```
   https://<ums_server>:8443/ums_filetransfer/avaya-agent.inf
   ```

   Note:

   Replace <ums_server> with the FQDN or IP Address of the UMS Server.

3. Start the UMS Console and log in by using the login and password credentials which were previously recorded.
4. Import the profile that is, profiles.zip into the UMS by using: **System—> Import—> Import Profiles**.

   The system displays the imported profile in UMS under **Profiles**.

5. Edit the profile and adopt the settings according to your environment under **System—> Firmware Customization—> Custom Partition—> Download**.

When editing the profile, the profile details must be typed in as follows:

- `https://<ums_server>:8443/ums_filetransfer/<cpname>.inf`
- Username: <ums-username>

- Password: <ums-password>

6. Upload the security certificates that require certificates, by using the IGEL UMS Console Files feature.
7. Right-click the file heading in UMS Console, and select **New File**.
8. By using UMS Console, associate the Avaya certificates and Avaya Agent profiles to the thin client.

Note:

In some cases, the thin client must be restarted after deployment of the Custom Partition.

Uninstalling Avaya Agent for Desktop on IGEL thin client using the IGEL UMS

Procedure

1. Start the Universal Management Suite (UMS) Console and log in by using the login and password credentials which were previously recorded.
2. Click the client that has **Avaya Agent** profile assigned to it.
3. Remove **Avaya Agent** object from **Assigned** object.
4. Right-click the client and select **Update**.

Downgrading Avaya Agent for Desktop

Procedure

1. The following Avaya Agent for Desktop's profile directory or folder are removed:

- For Windows: `%AppData%\Avaya\Avaya Agent`
- For Linux: `/etc/avaya-agent/userName`
- For Mac: `/Users/userName/Library/Preferences/avaya-agent`

2. If the installation was customized for different properties, such as log directory, those folders must also be deleted. This detail will be left as an activity for the admin.
3. Uninstall Avaya Agent for Desktop for the following.
   a. Windows: Go to **Control Panel** → **Programs and Features** → **Avaya Agent**. Click **Uninstall**.

b. Linux (RPM package), use the following commands:
   - `rpm -e avaya-agent`;
   - if "`rpm -e`" gets error "specifies multiple packages", then execute the following: **`rpm -e --allmatches avaya-agent`**;

c. Linux (DEB package), use the following commands:
   - **`sudo dpkg -r avaya-agent`**

d. Mac: Move Avaya Agent for Desktop from the application folder to trash.

4. Agents must then follow the initial Avaya Agent configuration flow.

Chapter 5: Component configuration

Assigning functions to buttons in Avaya Aura® Communication Manager

About this task

To assign buttons to the feature buttons in the Avaya Agent for Desktop user interface, perform the following actions.

Warning:

If you do not configure the feature buttons, then the application displays an error 'required features not found – offline', and you cannot sign in as an agent. Configuring the feature buttons is required to sign in the agent in Avaya Agent for Desktop.

Procedure

1. Log in to the Avaya Aura® Communication Manager administration interface.

   You can choose to log in to the Station Administration Terminal (SAT) on Avaya Aura® Communication Manager.

2. In the text input field, type the following command:

   `change station XXXXX`, where `XXXXX` is the station ID that corresponds to the agent extension number to be used with Avaya Agent for Desktop.

   The system navigates to specific station administration form based on the provided station ID.

3. Navigate to pages 4 and 5 and assign buttons for the following functions:
   - Manual in: `manual-in`
   - Auto in: `auto-in`
   - After call: `after-call`
   - Aux work: `aux-work`
   - Release: `release`

     Note:

     The release function button is required for only H.323 station.

- Three buttons for call appearances: `call-appr`
- (Optional) A button for displaying Vu statistics: `vu-display Fmt:1 ID:32`

  Note:

  Stats Console is an optional feature and requires additional administration. See the *Avaya Contact Center Administration* documentation for more information.
- A button for displaying Q-stats which shows the statistics of calls in a queue for a station: `q-calls`.

Assigning functions to buttons for SIP users in Avaya Aura® System Manager

About this task

To assign buttons to the feature buttons in the Avaya Agent for Desktop user interface for SIP users in Avaya Aura® System Manager, perform the following actions.

Warning:

If you do not configure the feature buttons, then the application displays an error 'required features not found – offline', and you cannot sign in as an agent. Configuring the feature buttons is required to sign in the agent in Avaya Agent for Desktop.

Procedure

1. Login into the Avaya Aura® System Manager application.
2. Navigate to **User Management** > **Manage users** > **New User Profile** > **Communication Profile** > **CM Endpoint Profile** > **Endpoint Editor**.
3. In the **Template** field, select the required station type.

   Note:

   Though Avaya Agent for Desktop supports 9608 SIPCC, 9641 SIPCC, 9621 SIPCC, 9611 SIPCC and J179CC for SIP, note that, for SIP shared control mode when Avaya Agent for Desktop is in desk phone mode with Avaya one-X® Agent, you must use station type as 9608SIPCC only.
4. At the bottom of the page, click the **Button Assignment** tab.
5. On the **Main Buttons** tab, assign buttons for the following functions:
   - Manual in: `manual-in`
   - Auto in: `auto-in`
   - After call: `after-call`
   - Agent login: `agent-login`

- Auxiliary work: `aux-work`
- Three buttons for call appearances: `call-appr`
- (Optional) A button for displaying Vu statistics: `vu-display`
- (Optional) A button for displaying Q-stats which shows the statistics of calls in a queue for a station: `q-calls`

Note:

For more information about managing SIP users in Avaya Aura® System Manager, refer the *Managing Users* section of the *Administering Avaya Aura® System Manager guide*.

Configuring Avaya Agent for Desktop for Avaya Oceana Solution

About this task

Use the following procedure to configure systems required for using Avaya Agent for Desktop with Avaya Oceana® Solution.

Before you begin

- Ensure that Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Enablement Server (AES), and Avaya Aura® Communication Manager is configured with Avaya Control Manager (ACM).
- LDAP is in active state and is configured to work with Avaya Aura® System Manager.

Procedure

Configuring a new agent

1. If you have added new members to LDAP, you must synchronize LDAP with Avaya Aura® System Manager. Do the following:
   a. Login to Avaya Aura® System Manager.
   b. Go to **Directory Synchronization** > **Active Synchronization Jobs**.

      The system displays the User Synchronization window.
   c. Click **Create New Job**.

      The system displays the New User Synchronization Job window.
   d. Click **Run Job** without changing any settings.

      The system displays the Synchronization Job Summary screen after the process is completed.

Checking Avaya Aura® Communication Manager stations

Note:

If you are creating a voice user, you must create a station.

2. To check or add a new station on Avaya Aura® Communication Manager, do the following:
   a. Login on Avaya Aura® Communication Manager.
   b. Run the following command and choose `w2ktt`: **`sat`**.
   c. To check whether a station exists, for example 6022011, run the following command: **`list station 6022011`**.
   d. If the station does not exist, you must create a new station using the following command: **`add station next`**.
   e. Set the station name and password and press Esc-E to save the details.
   f. Run the following command to mark the new station details as permanent: **`save translation`**.

      The station details are added successfully.

      Note:

      If you are using SIP, you must create a station on Avaya Aura® System Manager.

Adding a new agent on Avaya Aura® Communication Manager

Note:

For creating agent skill, vector, and VDN must be available on Avaya Aura® Communication Manager.

3. To add an agent on Avaya Aura® Communication Manager, do the following:
   a. Run the following command to add a new agent: **`add agent-loginID next`**.
   b. Define agent name and password and press Esc-E to save the details.

Creating an agent on Avaya Control Manager (ACM)

4. To create an agent on ACM, do the following:
   a. Login on ACM.
   b. On the **User Management** screen, click the required site name to view the list of users.
   c. Click the add icon on top-right of the screen.

      Note:

      If the add button is displaying on top-left of the screen, then there is something wrong with the browser version you are using; ACM will not work properly in this case.

   d. Select the **Avaya Oceana** or **Workspaces for Elite** depending on your environment on the bottom of the screen.

This will enable the domain details for LDAP users.

e. Add details in the following fields:

- **First Name**: For example: Team2 or T2
- **Surname**: For example: A<agent number> or A11
- **Profile**: Use the default value.
- **LDAP username**: For example: <team number><agent number>
- **Authentication Type**: Use the default value.
- **Domain**: Use the default value.
- **Username**: For example: <team number><agent number>@<ACM server domain name>.
- **Password**: Define password. Oceana Workspaces uses LDAP password, so this password does not affects it.
- **Confirm Password**: Same as the newly defined password.
- **Force password reset on next login**: Keep this as unchecked.
- **Avaya login**: For example : 6021011
- **Team**: For example: SalesTeam
- **Template**: Use the default value.
- **Description**: Use the default value.
- **Email**: Use the default value.
- **SIP URI**: Use the default value.
- **Communication Profile Password**: Use the default value.
- **Confirm Communication Profile Password**: Use the default value.
- **Extension**: For example: 6022011

f. Click **Save**.

Note:

After you create agent on ACM, the agent is also created on Avaya Aura® Communication Manager. You must save the translation again on Avaya Aura® Communication Manager.

g. On the **Permissions** tab, select the required **Role** for the agent.

h. On the **Avaya Oceana** tab, select the channels and the supervisor details.

i. On the **Attributes** tab, select the agent attributes to filter the contacts.

Note:

Always select the attribute team for your team.

Avaya Control Manager Synchronization

Note:

If Avaya Control Manager notifies that the agent end point does not exists and you know it does, then you must manually synchronize Avaya Control Manager with Avaya Aura® Communication Manager.

5. To synchronize Avaya Control Manager, do the following:
   a. Login into Avaya Control Manager Windows server.
   b. Launch the Avaya Synchronizer application.
   c. In the **Objects to synchronize** field, deselect all except **Extension**.
   d. Click **Start**.

Configuring and using Avaya Agent for Desktop with Oceana Workspaces

6. To configure and use Avaya Agent for Desktop with Oceana Workspaces, do the following:
   a. Launch Avaya Agent for Desktop application.
   b. Go to the **Settings** window.
   c. On the **Settings** tab, click the **Server** menu.
   d. Select the required options for the following sections:
      - **Avaya Control Manager Settings**
      - **License Server Settings**
      - **Local Server Settings**
   e. Click **Save**.
   f. Restart the Avaya Agent for Desktop Application.
   g. Once the Avaya Agent for Desktop application is launched, login with station details only.
   h. Launch Oceana Workspaces in a browser window.
   i. Provide **Username** and **Password** and click **SIGN IN**.
   j. On the **Activate Agent** screen, click **Activate**.

      The Oceana Workspace window is launched.
   k. Click **Start Work**.

      The Oceana Workspace application will synchronize and start working with the **Avaya Agent for Desktop** application.

Session Manager survivability for SIP signaling

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.

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 Agent for Desktop cannot connect to the primary Session Manager, Avaya Agent for Desktop automatically fails over to the secondary Session Manager without user intervention. This is to ensure service continuity for Avaya Agent for Desktop users. If failover occurs while a user is on an active call, Avaya Agent for Desktop attempts to maintain the speech path and signaling for call control. If primary Session Manager is available again, Avaya Agent for Desktop will not switch back to primary Session Manager while there is an active or held call.

Chapter 6: Initial administration

Familiarizing with the Avaya Agent user interface

Settings menu

Settings menu search functionality

In Avaya Agent for Desktop 2.0, the previous **Configuration** menu is renamed to **Settings** menu and the user interface has also been enhanced. In the new **Settings** menu window, you can either navigate to a required settings screen or you can also search the settings option with a search keyword in the **Search** field. Using the search filter takes you directly to the searched settings list. On this new window, you can either view all settings together or browse and navigate to menu option for each tabs. The available tabs are: **Settings**, **Reason Codes**, **Greetings**, and **Screen Pop**. For each tab, there are menu options in the left pane. Clicking a menu option displays the respective menu details on the right pane.

Chapter 7: Settings configuration

Server menu field descriptions

Important:

If you make any changes in the Settings window and if a red label *The changes require Application restart* is displayed at the bottom of the Settings window, then you must restart the Avaya Agent for Desktop application.

Avaya Control Manager Settings:

Note:

When using Avaya Control Manager , the other screens from the Avaya Agent for Desktop Settings window are inaccessible until you provide an address for Avaya Control Manager.

Name	Description
AAFD Login Type	The available options are: • **ACM Unified Login**: ACM Unified Login option allows you to enforce the use of ACM when ACM is selected as the login option. If this option is enabled and there is an ACM login failure, the Avaya Agent for Desktop application goes back to the ACM Login window. • **Single Sign-On ACM Login**: Single Sign-On ACM Login option in Avaya Agent for Desktop allows you to use SSO to download user configuration from ACM. This feature works only on Windows platform. On other platforms, the SSO setting is skipped. The agent must login only once on the system containing the Avaya Agent for Desktop application and does not need to login into Avaya Agent for Desktop separately. Also, ACM and Avaya Agent for Desktop must be on the same domain. **Note:** The Single Sign-On ACM Login feature is not available for Mac systems. • **Basic ACM Login**: Basic ACM Login option works in a similar way as it was working in the earlier versions of Avaya Agent for Desktop for ACM mode. **Note:** When multiple templates are assigned to a user in ACM Web portal, the user can select different ACM template using the ACM Profile field while login on Avaya Agent for Desktop. This feature is available for all ACM login types except **Use Local Configuration** and **AADS Login** login types on Avaya Agent for Desktop. When a user selects an ACM template and clicks the **Select Profile** button on Avaya Agent for Desktop, the configurations for selected ACM template is downloaded and ACM login is completed. A user must select an ACM profile within two minutes to select template for the ACM login. If during this time interval ACM template is not selected, ACM login is aborted and you get logged out. Offline messages are displayed as ACM login status.

Table continues…

Name	Description
	If for a selected user only one template is configured on the ACM Web portal, ACM login does not require any actions from the user to select a profile. In this case, template name is shown in the ACM Profile field, but ACM Profile field and Select Profile buttons are not available for a user for selection. In the Basic ACM Login and Unified ACM Login types, users have option to logout of ACM. There is only one difference between Basic ACM Login and Unified ACM Login types, that is, if Unified ACM Login type is selected, user cannot change station and agent login credentials manually. When Unified ACM Login type is used, input fields for Station ID, Agent ID, login mode, and passwords is disabled for the user. ACM Logout functionality provides ability to change ACM login credentials or profile name and re-login on Avaya Agent for Desktop. When ACM logout is completed, all settings, which has been downloaded through ACM, is resetted to default, and input fields for ACM login credentials is available for the user. • **Use Local Configuration**: When the **Use Local Configuration** option is selected, the agent profile uses the configuration defined on the local system. Supports both H.323 and SIP signalling. • **AADS Login**: When this option is selected, Avaya Agent for Desktop retrieves configuration details and login credentials using the external Avaya Aura® Device Services (AADS) configuration server. There are following two ways to login on to Avaya Aura® Device Services server using Avaya Agent for Desktop: - **Basic authentication**: Here, Avaya Agent for Desktop requests agents to provide the email address or AADS server direct URL of the third-party service. The AADS server sends back the configuration details if the login details are entered correctly. On next step, user needs to provide AADS login and password on Avaya Agent for Desktop main login window. - **Third-party authentication using OAuth2 SAML**: Here, Avaya Agent for Desktop requests

Table continues…

Name	Description
	agents to provide the email address or AADS server direct URL of the third-party service. Once inputs are provided, Avaya Agent for Desktop redirects agents to third-party login screen. On next step, user needs to provide login and password on third-party login screen. This is implemented using the OAuth2 protocol and Security Assertion Markup Language (SAML) authentication method. **Preferred AADS SAML login type user experience:** • **Preferred SAML login type is active**: When **AAFD Preferred SAML login type** check box is selected, AADS login is changed to "`bearer`" forcibly even if service supports "basic" sign in. So, user can enter URL without specific `?preferredAuth=bearer` add-on to the initial request URL. If `bearer` sign in fails, user can perform `basic` sign in. The same algorithm is applied to e-mail user input type sign in. • **Preferred SAML login type is inactive**: When **AAFD Preferred SAML login type** is not selected, and `?preferredAuth=bearer` is not there in the user input URL, then sign in is successful with correct AADS credential. If service supports "basic" sign in, but `?preferredAuth=bearer` is there in the user input URL, then sign in fails. **AAFD Preferred SAML use cases:** • The AADS login is successful when Preferred SAML flag is set to active with URL with `?preferredAuth=bearer`. • The AADS login is successful when Preferred SAML flag is set to active with URL without `?preferredAuth=bearer` in address, but server supports `bearer` sign in. • The AADS login is successful when Preferred SAML flag is set to active with e-mail. • The AADS login is successful when Preferred SAML flag is set to active with SAML URL, but server does not support SAML.

Table continues…

Name	Description
	Note: In case of the AADS login, the settings are configured by the administrators on the AADS server and applied during the login to AADS, but local user settings are still in use if it is not overwriten by server values. After AADS logout, user's local settings are restored back for all parameters, except those which require reboot.
Primary ACM Address URL	The field to configure the primary Avaya Control Manager address. This field is inactive if the **Use Local Configuration** check box is selected.
Secondary ACM Address URL	The field to configure the secondary Avaya Control Manager address. This field is inactive if the **Use Local Configuration** check box is selected. The system uses the secondary Avaya Control Manager address if the primary server is unavailable.

License Server Settings:

Name	Supported signalling	Description
License server URL	Both H.323 and SIP	The URL to connect to the WebLM licensing server. The format of the URL must be the following: `https://<WebLMhost>:<port>/WebLM/LicenseServer` where: • `<WebLMhost>` is the host name or IP address of the WebLM server. • `<port>` is the port used for connecting to the WebLM server.

Local Server Settings:

Name	Supported signalling	Description
Signalling	SIP or H.323	Select the signalling option you want to use for the Local Server Settings.
Primary CM address	H.323	The field to configure the IP address of the primary Avaya Aura® Communication Manager server.
Secondary CM address	H.323	The field to configure the IP address of the secondary Avaya Aura® Communication Manager server. The system uses the secondary Avaya Aura® Communication Manager address if the primary server is unavailable.
Primary SIP Proxy address	SIP	The field to configure the IP address of the primary SIP proxy server. Select one of the following values: • **TCP** • **TLS** • **UDP** **Note:** If you are using Avaya Agent for remote agent through session border controller (SBC), you must type **Primary SIP Proxy address** as Primary SM External SBC interface IP Address.

Table continues…

Name	Supported signalling	Description
Secondary SIP Proxy address	SIP	The field to configure the IP address of the secondary SIP proxy server. The system uses the secondary SIP proxy address if the primary server is unavailable. Select one of the following values: • **TCP** • **TLS** • **UDP** **Note:** If you are using Avaya Agent for Desktop remotely through session border controller (SBC), you must type **Secondary SIP Proxy address** as Secondary SM External SBC interface IP Address.
SIP domain	SIP	The field to configure the domain name for SIP.

Table continues…

Name	Supported signalling	Description
Number of connection attempts	Both H.323 and SIP	The field to configure the number of connection attempts before closing the session if the system cannot establish a connection to Avaya Aura® Communication Manager. When Avaya Agent for Desktop makes an attempt to connect to Avaya Aura® Communication Manager (CM), Avaya Agent for Desktop tries to connect to the primary CM server, and if the connection cannot be established, Avaya Agent for Desktop tries to connect to the secondary CM server, if a connection to a secondary CM server is configured. The process of unsuccessfully trying to connect to one or two CM servers is considered a failed connection attempt. If the number of connection attempts is exceed, Avaya Agent for Desktop displays a notification to the user. If the connection to either one of the CM servers is established, the CM server is provided with an Alternate Gateway List (AGL) that is associated with the network region.
CM Auto Answer Support Required	H.323	Select this option if your administrator has configured the extension on Avaya Aura® Communication Manager to support Auto Answer.
Communication Manager Onhook Dialing Support Required	H.323	This setting must be enabled when "Onhook dialing on Terminal" is set to Y on Avaya Aura® Communication Manager.

Related links

Configuring the connection to Avaya Control Manager on page 87
Configuring the WebLM license URL for H.323 and SIP on page 88
Configuring the connection to Avaya Aura Communication Manager on page 89

Configuring the connection to a SIP proxy server on page 90
SIP shared control mode overview on page 91
Configuring the directory settings for H.323 and SIP on page 94

Configuring the connection to Avaya Control Manager

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

About this task

The agent profiles can be managed locally using Avaya Aura® Communication Manager or using Avaya Control Manager.

This procedure describes how to configure Avaya Agent for Desktop to function using Avaya Control Manager.

You can configure the connection to a secondary Avaya Control Manager server, if a secondary server is available. The system uses the secondary Avaya Control Manager address if the primary server is unavailable.

Procedure

1. In the Avaya Agent for Desktop Settings window, click the **Server** tab.
2. In the **AAFD Login Type** field, select any of the following options:
   - **ACM Unified Login**: ACM Unified Login option allows you to enforce the use of ACM when ACM is selected as the login option. If this option is enabled and there is an ACM login failure, the Avaya Agent for Desktop application goes back to the ACM Login window.
   - **Single Sign-On ACM Login**: Single Sign-On ACM Login option in Avaya Agent for Desktop allows you to use SSO to download user configuration from ACM. This feature works only on Windows platform. On other platforms, the SSO settings is skipped.
   - **Basic ACM Login**: Basic ACM Login option works in a similar way as it was working in the earlier versions of Avaya Agent for Desktop for ACM mode.
3. In the **Primary Avaya Control Manager URL**, type the **Primary Avaya Control Manager URL**.
4. (Optional) In the **Avaya Control Manager Settings** field, type the **Secondary Avaya Control Manager URL**.
5. Click **Save**.
6. Restart the Avaya Agent for Desktop application.

Related links

Server menu field descriptions on page 79

Configuring the WebLM license URL for H.323 and SIP

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

About this task

Avaya Agent for Desktop needs a valid WebLM license to function.

Important:

In Avaya Agent for Desktop, you can now avail a trial period of 30 days for using Avaya WebLM license.

This procedure describes how to configure Avaya Agent for Desktop for H.323 and SIP to connect to the WebLM server.

Procedure

1. In the Avaya Agent for Desktop Settings window, click the **Server** tab.
2. **(Optional)** In **AAFD Login Type**, select **Use Local Configurations**.
3. **(Optional)** In **Local Server Settings**, click one of the following options:
   - **H.323**: If H.323 signaling type is used, Avaya Agent for Desktop must be restarted after the notification to apply the parameters.
   - **SIP**: If SIP signaling type is used, Avaya Agent for Desktop will start working after a valid License server URL is configured. You do not need to restart the Avaya Agent for Desktop application.

   The system displays the screen based on the option selected .
4. In the **License server URL** field, enter the URL to connect to the WebLM server.

   The format of the URL must be the following:

   ```
   https://<WebLMhost>:<port>/WebLM/LicenseServer
   ```

   where:

   - `<WebLMhost>` is the host name or IP address of the WebLM server.
   - `<port>` is the port used for connecting to the WebLM server.
5. Click **Save**.
6. Restart the Avaya Agent for Desktop application.

Related links

Server menu field descriptions on page 79

Configuring the connection to Avaya Aura® Communication Manager

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

About this task

The agent profiles can be managed using Avaya Aura® Communication Manager (CM) or using Avaya Control Manager.

This procedure describes how to configure Avaya Agent for Desktop to function using Avaya Aura® Communication Manager.

You can also configure the connection to a secondary Avaya Aura® Communication Manager server, if a secondary server is available. The system uses the secondary Avaya Aura® Communication Manager address if the primary server is unavailable.

Note:

If you install Avaya Agent for Desktop on HP thin clients, disable media shuffling on Avaya Aura® Communication Manager, in the IP Network Region configuration menu.

Procedure

1. In the Avaya Agent for Desktop Settings window, click the **Server** tab.
2. In **AAFD Login Type**, select **Use Local Configurations**.
3. In **Local Server Settings**, select **H.323**.
4. In the **Primary CM address** field, enter the IP address of the primary Avaya Aura® Communication Manager server.
5. (Optional) In the **Secondary CM address** field, enter the IP address of the Enterprise Survivable Server (ESS or Survivable core server).

   Note:

   When the primary Communication Manager server goes down, the current Avaya Agent implementation automatically registers the station with ESS. During this time, if any agent tries to register on the primary Communication Manager server, the agent automatically gets registered on ESS. This setup helps in continuing an ongoing call, until the agent drops the call. Once the call is dropped, the agent gets registered in aux mode. After the Communication Manager server recovery, the agent must log off and login again to establish an error free connection.
6. In the **Number of Connection Attempts** field, type the number of connection attempts that Avaya Agent for Desktop can perform while initiating the connection to Avaya Aura® Communication Manager.

When Avaya Agent for Desktop makes an attempt to connect to Avaya Aura® Communication Manager (CM), Avaya Agent for Desktop tries to connect to the primary CM server, and if the connection cannot be established, Avaya Agent for Desktop tries to connect to the secondary CM server, if a connection to a secondary CM server is configured. The process of unsuccessfully trying to connect to one or two CM servers is considered a failed connection attempt.

If the number of connection attempts is exceed, Avaya Agent for Desktop displays a notification to the user.

If the connection to either one of the CM servers is established, the CM server is provided with an Alternate Gateway List (AGL) that is associated with the network region.

7. Click **Save**.
8. Restart the Avaya Agent for Desktop application.

Related links

Server menu field descriptions on page 79

Configuring the connection to a SIP proxy server

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

About this task

Use this procedure to configure the connection to the primary server in Avaya Agent for Desktop.

You can also configure the connection to a secondary SIP proxy server if a secondary server is available. The system uses the secondary SIP proxy server address when the primary server is unavailable.

Procedure

1. In the Avaya Agent for Desktop Settings window, click the **Server** tab.
2. In **AAFD Login Type**, select **Use Local Configurations** to enable the local storage of the agent's information.
3. In **Local Server Settings**, ensure that **SIP** is selected.
4. In the **Primary SIP Proxy address** field, type the IP address of the primary SIP proxy server.

   Note:

   If you are using Avaya Agent for remote agent through session border controller (SBC), you must type **Primary SIP Proxy address** as Primary SM External SBC interface IP Address.

5. In the corresponding fields, specify the port number and the port type.

Note:

The port number for **TCP** and **UDP** ports is `5060`. The Port number for **TLS** port is `5061`.

6. In **SIP domain**, type the SIP domain.

   Note:

   Without the SIP domain, you cannot register on the SIP proxy server.

7. **(Optional)** In the **Secondary SIP Proxy address** field, type the IP address of the secondary SIP proxy server.

   Note:

   If you are using Avaya Agent for Desktop remotely through session border controller (SBC), you must type **Secondary SIP Proxy address** as Secondary SM External SBC interface IP Address.

8. **(Optional)** In the corresponding fields, specify the port number and the port type.
9. In the **Number of Connection Attempts** field, type the number of connection attempts that Avaya Agent for Desktop can perform while starting the connection to the SIP proxy server.
10. Click **Save**.
11. Restart the Avaya Agent for Desktop application.

Related links

Server menu field descriptions on page 79

SIP shared control mode overview

This feature provides users ability to direct media to a desk phone or a hard phone while issuing signaling commands from the desk phone and/or from the Avaya Agent for Desktop application. A Spark-based shared signaling channel is established between the controlling client; that is Avaya Agent for Desktop, and the controlled client; that is a desk phone, through Avaya Aura® Session Manager. This connection keeps the call states in sync and communicates the signaling messages properly.

This feature deals with two main entities, controlled client; that is Avaya SIP endpoints that support SIP shared control mechanism and controlling client; that is Avaya Agent for Desktop client application.

The following functions are performed through an endpoint or a hard phone:

- Handle a call
- Handle a conference
- Manage other contact center agent features

The following functions are performed through Avaya Agent for Desktop client application:

- Registration
- Subscription other than the dialog package
- Manage contacts
- Manage call logs

Note:

The following are few current limitations in using SIP shared control mode in Avaya Agent for Desktop:

- This feature is available only when the controlling client and the controlled device use the TLS transport protocol.
- Currently, Avaya Aura® Session Manager is the only Avaya registrar that supports the q-value 0 registration mechanism. When an endpoint registers with q-value 0, Avaya Aura® Session Manager does not provides the incoming requests to the endpoint regardless of how many other endpoints are registered on behalf of the same Address of Record (AOR).
- The Coaching feature works in shared control mode only.

Feature interaction

The following features are done through the slave endpoint:

- Call handling
- Conference handling
- Agent features
- Remote mute

The following features are done directly through Avaya Agent for Desktop:

- Registration Subscription (apart from dialog package)
- Contacts
- Call logs

Remote Mute

The user has an ability to mute remote device in a shared control mode.

- When the user in shared control clicks on the mute button, the mute button blinks until it is answered by the slave device.
- The Disable headset mute button is supported in a shared control mode.
- Avaya Agent for Desktop as a master device requests the current mute state on the slave device side when the shared control session is established.
- The remote microphone button is disabled when the mute button is blinking while Avaya Agent for Desktop waits for the slave device response.

. .

Limitations

The following are the current limitations in SIP Shared Control for Avaya Agent for Desktop:

- This feature is available only if the master client and the slave device is used in TLS protocol.
- Currently Session Manager is the only Avaya registrar that supports the q-value 0 registration mechanism. When an endpoint registers with q-value 0, Session Manager knows not to offer incoming requests to that endpoint regardless of how many other endpoints are registered on behalf of the same Agent Owned Recalls (AOR).
- The Call Appearance information, for example - display name or number, can be different between the slave and the master devices during a transfer or a conference call creation. The slave device does not get any information if a master device initiates a transfer or a conference call. Only sessions are updated when the process is completed.

Related links

Server menu field descriptions on page 79
Configuring Avaya Agent for Desktop for using SIP shared control mode on page 93
Configuring Avaya Agent for Desktop for using SIP shared control mode with J179 hardphone on page 94

Configuring Avaya Agent for Desktop for using SIP shared control mode

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

About this task

To use Avaya Agent for Desktop in shared control mode, you must switch the transport type for primary and secondary SIP proxies to TLS and set 5061 as the port number.

Procedure

1. In the Avaya Agent for Desktop Settings window, click the **Server** tab.
2. In **AAFD Login Type**, select **Use Local Configurations** to enable the local storage of the agent's information.
3. In **Local Server Settings**, ensure that **SIP** is selected.
4. In the **Primary SIP Proxy address** field, type the IP address of the primary SIP proxy server.

   Note:

   If you are using Avaya Agent for remote agent through session border controller (SBC), you must type **Primary SIP Proxy address** as Primary SM External SBC interface IP Address.
5. In the corresponding fields, select the port type as **TLS** and port number as 5061.
6. In **SIP domain**, type the SIP domain.
7. Click the **Preferences** tab.

8. In the **Login Mode** area, click and select the **Desk Phone** option as a **Login mode**.
9. Click **Save**.
10. Restart the Avaya Agent for Desktop application.

Related links

SIP shared control mode overview on page 91

Configuring Avaya Agent for Desktop for using SIP shared control mode with J179 hardphone

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

Procedure

1. In the Avaya Agent for Desktop Settings window, click the **Server** tab.
2. In **AAFD Login Type**, select **Use Local Configurations** to enable the local storage of the agent's information.
3. In **Local Server Settings**, ensure that **SIP** is selected.
4. In the **Primary SIP Proxy address** field, type the IP address of the primary SIP proxy server.

   Note:

   If you are using Avaya Agent for remote agent through session border controller (SBC), you must type **Primary SIP Proxy address** as Primary SM External SBC interface IP Address.
5. In the corresponding fields, select the port type as **TLS** and port number as .
6. Click the **Preferences** tab.
7. In the **Login Mode** area, click and select the **Desk Phone** option as a **Login mode**.
8. Click **Save**.
9. Restart the Avaya Agent for Desktop application.

Related links

SIP shared control mode overview on page 91

Configuring the directory settings for H.323 and SIP

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

About this task

Public Directory provides access to corporate or public directory services. It functions as Lightweight Directory Access Protocol client (LDAPv2 or LDAPv3). You must first create and configure the service with Avaya Agent for Desktop to import or search a contact in the public directory (LDAP).

Procedure

1. On the Directory tab, in the **Directory Address** and **Directory Port** fields, enter the URL of the network domain or the IP address and the port of the public directory server.
2. In the **Directory search root** field, enter an LDAP format string representing an information type.

   To configure the **Directory Root Search** field correctly, you must obtain the LDAP format string according to the configuration of the LDAP server.

   For example, `ou=people, o=mycompany.com` specifies that information under the organization unit of people within the organization of *mycompany.com* is used for the search. For information on Base DN or Search Root strings, see the documentation for your LDAP system and company database configuration.
3. In the **Directory Username** field, enter the user name to connect to the public directory server.

   Provide a user name only if the public directory server requires authorization.
4. In the **Directory Password** field, enter the password for the user specified in the **Directory username** field.

   If you are unsure of the settings for your Public Directory server, contact the administrator of that system.
5. In the **Directory bind option** field, select the LDAP service type. Choose one of the following options:

   - Simple: to interface the directory service with an LDAPv2 server
   - GSS: to interface the directory service with an LDAPv3 server

   The GSS bind option is not supported on MAC and Linux systems.
6. Click **Save**.

   Note:

   For the changes to the LDAP settings to take effect, restart Avaya Agent for Desktop.
7. Restart the Avaya Agent for Desktop application.

Related links

Server menu field descriptions on page 79

Preferences menu field descriptions

Agent Settings:

Name	Description
Ready Mode	Use the following options to configure the Avaya Aura® Communication Manager Ready Mode settings: • **Auto-in**: Overrides **Manual In**, the default Avaya Agent for Desktop call handling. To limit the time that the agent spends in the **After Call Work** state, use this option in combination with the **Communication Manager timed after the call work** feature. The **Auto-in mode** option is not equivalent to the **CM Auto Answer Support Required** option. • **Manual-in**: The default setting. You must ensure that the **Manual In** option is in the assigned state for the Avaya Agent for Desktop program to perform the work.
Timed After Call Work	Select to provide the number of seconds in the seconds field to set a limited time for the **After Call Work Duration (seconds)** feature. After the configured time expires, you can leave the After Call Work state and become ready to take calls. Keep the **Timed After Call Work** check box clear to make the **After Call Work Duration (seconds)** time unlimited.
Allow Manual Call After Work	Select to change to the After Call Work state manually.

Common:

Name	Description
Automatically Log In The Agent	Log automatically to the user on ACD after successfully registering the extension with Avaya Aura® Communication Manager. If the **Automatically log in agent** check box is clear, the system only registers the station extension and you must register the agent manually. The system also displays the **Automatically log in agent** check box in the login dialog box.

Table continues…

Name	Description
Automatically Log In The Station	Log automatically on the station once the application is launched.
Launch Avaya Agent When Windows start	Select this option to automatically launch the Avaya Agent for Desktop application on your Windows system start up.
Show User Interface	The system hides the user interface to facilitate Managed Control mode. You can re-enable the display of the user interface by right-clicking the Avaya Agent for Desktop icon in the system tray and deselecting **Hide Interface**.
Always Display The Main Window On Top	Select this option to keep the main Avaya Agent for Desktop application on top of your screen windows.
Local Auto Answer	To use this option for Avaya Agent for Desktop, you need to ensure that the **Auto answer** is disabled on Avaya Aura® Communication Manager. You can use **Local Auto Answer** or Avaya Aura® Communication Manager **Auto answer**, but not both. The **Local Auto Answer** option is designed to provide the end user ability to change the workflow on the fly without making changes on Avaya Aura® Communication Manager.
Stay In Notification Area If Main Window Is Closed	Select this option if you want to keep the closed main window active in the Taskbar notification area.
Show WebLM Server Warning Messages	Select this option to enable the warning message alerts from the WebLM server.

Login Mode:

Name	Description
Login mode	Avaya Agent for Desktop supports the following login modes: • **My Computer**: Use this option to use Avaya Agent for Desktop with general capabilities on your computer. • **Desk Phone**: Use this option for controlling another instance of the Avaya Agent for Desktop in a shared control mode. **Note:** You must use port type as TLS for using Desk Phone login mode. Additionally, if you use this mode, the **Audio** tab in the **Settings** window is disabled. • **Other Phone**: Use this option to use the Avaya Agent for Desktop in a Telecommuter mode. You need to define the telecommuter or **Other Phone Number** once you select this option. **Note:** If you are logging to Avaya Agent for Desktop with Other Phone Mode using 10 digit extension, you must set the dialing rules Internal extension length to 10 for successful login attempt. If these lengths are not same, the login attempt will fail and an error is displayed. Additionally, if you use this mode, the **Audio** tab in the **Settings** window is disabled. **Note:** Telecommuter mode has the following limitations: - Auto answer is not supported. The server waits when the TC device answers the call. In this case, Avaya Agent for Desktop cannot answer the call. - The ability to check the availability of the TC device during login is not present for H323 signaling. An agent remains logged in even if TC device is not logged in. The availability check for TC device occurs through a call. In H.323 protocol, we do not receive an

Table continues…

Name	Description
	update of the call state, until the call is processed that is, if it is cleared or adopted on the other side, or until the call is not be dropped on the server. - Greeting is not supported. An audio path is established between the TC device and caller. In this case, Avaya Agent for Desktop does not participate in the audio transmission. This means, that greetings configured on Avaya Agent for Desktop are not playing on the caller's side.
Other Phone Number	The field to define the telecommuter or other phone number. For example, an office desk phone number or a mobile phone number. This field is active only for the Other Phone mode.
Check TC device To Login Agent	If this field is enabled, Avaya Agent for Desktop will login agent extension only after the call is answered on the mentioned **Other Phone Number** device.

Message Waiting Indicator:

Name	Description
Show Message Waiting Indicator	Select to activate the message waiting indicator.
Voice Mailbox Number	Enter the host agent **Voice Mailbox Number** as defined in the Avaya Aura® Messaging application.

DTMF:

Name	Description
DTMF Type	A field to select the DTMF type. The available options are: • **out-of-band** • **in-band** • **rtp-payload**
Comma Dialing Delay (msecs)	The dialing delay time if a comma is used in a dialed number.

Conference:

Name	Description
Use Consultative Type of Conference	A field to activate whether consultative conference should be followed or direct ones. In consultative conference, you need talk to the client first before creating the conference.

Transfer:

Name	Description
Use Consultative Type of Transfer	A field to activate whether consultative transfer should be followed or direct ones. In consultative transfer, you need talk to the client first before transferring the call.

Startup Message:

Name	Description
Startup Message	The message that Avaya Agent for Desktop displays as a disclaimer at startup.

The options for Avaya Agent for Desktop's **Agent state upon login** configuration parameter are as follows:

- Auxiliary - Avaya Agent for Desktop changes to auxiliary state right after a successful login, by using default aux reason code regardless of server settings. If there is a forced option for 'Aux Work Reason Code Type' configured on Communication Manager then Avaya Agent for Desktop may display an error 'Invalid reason code'.

  Note:

  The default reason code from Avaya Agent for Desktop settings is used, not the default reason code from Communication Manager.

- Ready - Avaya Agent for Desktop changes its state to ready right after a successful login, regardless of server settings.
- System Default - By default, Avaya Agent for Desktop reflects the agent state as is in Communication Manager. If the state is manual-in or auto-in, then Avaya Agent for Desktop stays in Ready state. If it is aux , then Avaya Agent for Desktop stays in Aux state with server default reason code.

  Note:

  The default reason code from Communication Manager settings is used, not the default reason code from Avaya Agent for Desktop.

  Note:

  For H.323 signaling, if there is no Aux feature button with Communication Manager default reason code configured for Avaya Agent for Desktop, then Avaya Agent for

Desktop stays in Aux mode with default reason code from Avaya Agent for Desktop settings, and not Communication Manager default reason code.

Avaya recomends to use the Communication Manager setting 'Work Mode On Login' and let Avaya Agent for Desktop's setting remain as default, to prevent potential errors and conflicts between Communication Manager and Avaya Agent for Desktop's settings.

Configuring the ready mode option

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

Procedure

1. On the **Settings** tab, click the **Preferences** menu.
2. In the Ready Mode field, select one of the following options:
   - **Auto-in**: Overrides **Manual In**, the default Avaya Agent for Desktop call handling. To limit the time that the agent spends in the **After Call Work** state, use this option in combination with the **Communication Manager timed after the call work** feature. The **Auto-in mode** option is not equivalent to the **CM Auto Answer Support Required** option.
   - **Manual-in**: The default setting. You must ensure that the **Manual In** option is in the assigned state for the Avaya Agent for Desktop program to perform the work.
3. Click **Save**.

Configuring the after call work settings

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

About this task

As an agent, you can enter the After Call Work state automatically or manually. The After Call Work time can also be limited or unlimited, depending on the configuration.

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Preferences** menu.

2. (Optional) In the **Agent Settings** field, perform the following actions to configure the timed After Call Work:
    a. Select the **Timed After Call Work** check box to limit the time that the system provides for After Call Work.
    b. In the text input field, enter the After Call Work time.
3. (Optional) In the **Agent Settings** field, select the **Allow Manual After Call Work** check box to switch to the After Call Work state manually.
4. Click **Save**.

Configuring the login settings

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

Procedure

1. In the Avaya Agent for Desktop Configuration window, click the **Preferences** tab.
2. In the **Message Waiting Indicator** area, select the **Show Message Waiting Indicator** check box to activate the message waiting indicator.
3. In the **Voice Mailbox Number** field, enter the appropriate voice mailbox number of the agent.
4. Click **Save**.

Configuring the Login mode settings

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

Procedure

1. In the Avaya Agent for Desktop Settings window, on the Settings tab, click the **Preferences** menu.
2. In the **Login Mode** field, select any one of the following options:
    - **My Computer**
    - **Desk Phone**
    - **Other Phone**

Note:

For more details about these fields, see the `Preferences tab field descriptions` section.

3. If you specify the **Login mode** as **Other Phone**, you must provide the agent's phone number in the **Telecommuter Number** field.
4. Click **Save**.

Configuring the comma dialing delay time

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

Procedure

1. On the **Settings** tab, click the **Preferences** tab.
2. In the **DTMF** section, in the **Comma Dialing Delay** field, type the delay time in seconds.
3. Click **Save**.

Configuring the transfer and the conference types

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

About this task

Avaya Agent for Desktop provides you with the possibility of making call transfers and conferences when you have an active call, as follows:

- Direct transfer: to transfer an active call to a contact in the contact center without announcing the transfer
- Consultative transfer: to speak to the contact before transferring the call
- Direct conference: to add the participants to the conference call without speaking to the participants
- Consultative conference: to speak to the participants before adding the participants to the conference call

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Preferences** menu.
2. Select the check boxes for the **Conference** and **Transfer** fields.

3. Click **Save**.

Note:

The limitation of Communication Manager conference is as follows:

Avaya Agent for Desktop generates a list of participants locally. If the participants are added by Avaya Agent for Desktop, then they are displayed in the list of participants.

However, if the context of conference is changed, that is, if someone is dropped or if someone adds another participant, then Avaya Agent for Desktop does not consider that local list of participants. As a result, Avaya Agent for Desktop stops showing the list of the participants.

Keeping the closed Avaya Agent for Desktop main window active in the Taskbar notification area

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Preferences** menu.
2. In the **Common** section, select the **Stay In Notification Area If Main Window Is Closed** check box to keep the closed main window active in the notification area.

Note:

- If this check box is in marked state, Avaya Agent for Desktop application will be kept in the notification area as tray icon when the main window is closed.
- If this check box is in unmarked state, the system will display a confirm quit dialog box “**Are you sure you want to quit?**” when the main window is closed.

3. Click **Save**.
4. Restart the Avaya Agent for Desktop application.

Configuring network and failover recovery

Procedure

1. In the Avaya Agent for Desktop, go to **Settings** tab, and click **Preferences**.
2. In the **Common** section, select the **Permanent Network Error Messages** checkbox.

   An agent receives notifications when Avaya Agent for Desktop is disconnected.
3. When Avaya Agent for Desktop is disconnected, you need to manually sign in if the network recovery time exceeds the configured number of seconds.

Note:

You can configure recovery time by going to **Preferences** → **Settings** → **Default Agent State** → **Agent State Recovery Timeout After Network Outage**.

4. If the network recovery time exceeds your configured time, the application displays a dialog box **Network Issue Detected Telephony Services not available**.
5. Click **OK** and log in manually.

   After signing in, the application displays a dialog box **Network Issue Resolved Telephony Services Restored**.
6. Click **OK**.

   Avaya Agent for Desktop restores you to your previous agent state.
7. If you want Avaya Agent for Desktop to automatically change the agent state after login, go to **Preferences** → **Settings** → **Default Agent State** → **Agent State Upon Login**.
8. Choose from the following:
   - **Ready**
   - **Auxiliary**
   - **Default**

   To know more about agent state upon login, refer to the information at the end of the topic Preferences menu field descriptions on page 96.

Invoking No Hold Conference feature

Before you begin

Do the following:

1. Select the **Use No Hold Type of Conference If Available** checkbox.
2. Clear the **Use Consultative Type of Conference** checkbox.

   Client must be in an active call for this task.

Procedure

You can do one of the following:

- To invoke the No Hold Conference feature from the **no-hold-conf** feature button, enter the number or extension to be dialed from conference button in the active call appearance.
- Or, from the **History** or **Contacts** widgets, right click the selected contact. Add the contact to the active call.

Using No Hold Type of conference

About this task

No Hold Conference is supported for SIP and H.323. Currently, No Hold Conference does not fully function on H.323. The H.323 limitations are as follows:

- For H323 station: No hold conference feature can be invoked only from the feature button. Users are not recommended to invoke this feature from Call appearance, Contact/History widget as a SIP station.
- Users can enter the desired extension while invoking No Hold Conference feature using the feature button on H.323, however the call still may be placed to another extension, which is configured on Communication Manager.
- The only indication of No Hold Conference process for H.323 is the feature button list indicator.
- No hold conference on the H.323 station does not have the "list of participants" and "drop last participant" features.
- Only one "Join" No Hold Conference call can be placed at the same time. If a user tries to invoke another No Hold Conference, then Avaya Agent for Desktop asks to cancel the previous "Join" call and initiate a new one.
- For shared control:
  - Connecting to #" message is not synchronized between devices. It is displayed only on No Hold Conference invoker side.
  - Avaya Agent for Desktop does not display the participant added by using No Hold Conference on J1xx side in the list of participants.
- The following limitation is for all stations: The No Hold Conference feature only lets the user send the call to an extension known to Avaya Aura® or Communication Manager, and not an external number.

Procedure

1. In the Avaya Agent for Desktop, go to **Settings** tab, and click **Preferences**.
2. In the **Conference** section, select the checkbox **Use No Hold Type of Conference If Available**.

   If the user selects the checkbox of the No Hold Conference, and the type of conference is not consultative, and if the no-hold-conf feature button is configured, then the active call is not put on hold while adding more users on the call.

   Users can use the no-hold-conf feature button to initiate No Hold Conference.

   Note:

   Error toast messages are displayed without affecting an active call when there are errors during escalating to No Hold conference.

Configuring No Hold type of transfer

Procedure

1. In Avaya Agent for Desktop, go to **Settings** tab, and click **Preferences**.
2. In the **Transfer** section, the following actions take place:
   a. If users clear the checkbox **Use No Hold Type of Transfer** Avaya Agent for Desktop sets both, the transferee and transfer's target sessions on hold, before sending the 'refer' message to start the transfer.
   b. If users select the checkbox **Use No Hold Type of Transfer**, then only one session is set in held state before the transfer starts.

      For the No Hold Transfer, Avaya Agent for Desktop uses the parameter USE_NO_HOLD_TRANSFER_TYPE.

Avaya Agent for Desktop supervisor feature overview

Avaya Agent for Desktop allows a supervisor to observe an agent's performance on any particular call, silently and unobserved. Avaya Agent for Desktop leverages only Communication Manager native capabilities for supervisor feature but in a user-friendly UI workflow. Here, a supervisor can listen-in or barge-in to the agent-customer interaction using this function. If the administrator has enabled this service, the observing icon appears as a work item on the supervisor's Avaya Agent for Desktop user interface. Additionally, Avaya Agent for Desktop Coaching feature now allows agents to listen to a supervisor and restrict customers from hearing the same conversation. The supervisor can activate this feature using the following options:

1. Contact numbers in the following sections:
   a. Call history
   b. Contact list
   c. Main screen input box
2. Right-click on the target agent row and select anyone of the following options:
   - **For H.323**

     Note:

     In this case, the functionality can be started by Station or Agent.

     a. Observe: listen-only: Supervisor could only hear the talk between the agent and the customer.
     b. Observe: listen/talk: Supervisor could also talk and the agent and the customer will hear the supervisor.
   - **For SIP**

Note:

In this case, the functionality can be started by Agent only.

a. Observe: listen-only: Supervisor could only hear the talk between the agent and the customer.

b. Observe: listen/talk: Supervisor could also talk and the agent and the customer will hear the supervisor.

c. Observe: Coaching: Only agent could hear the supervisor but the customer is restricted to hear the conversation.

Note:

In second case, only the Coaching button is allowed. Initially when coaching is activated, the session is started as listen-only and supervisor is muted. The supervisor could change the mode to listen-talk in a call appearance list after clicking on the corresponding button.

Avaya Agent Service Observing user Experience

1. You need to configure your extention with **sip-sobsrv** feature on System Manager.
2. You need to configure COR (class of restriction) which you would like to observe.
3. Login into the extention and make sure you have **sip-sobsrv** feature in "feature buttons" pad.
4. Also an agent should be logged in and be in **AUX** mode. You get notification if you try to use coaching feature in **Ready** mode.
5. You can also start Service Observing from Call Appearance

Enabling the supervisor feature from an existing database contact

About this task

There are two flows to enable this feature. In this flow, the coach can observe agents/VDNs that exists in the contact database. An agent must perform the following actions to enable the supervisor feature. You can also enable supervisor feature in a shared control mode.

Before you begin

For H.323, ensure that station and agent is logged in. For SIP, agent must be logged in and must be in an AUX state.

Procedure

1. Open the Contacts list.
2. Scroll-down or search the desired agent/VDN you want to coach.
3. Right-click on the target agent row and select anyone of the following options:
   - Observe: listen-only
   - Observe: listen/talk

- Observe: Coaching

Note:

- Avaya Agent for Desktop uses the feature button FAC in the background to activate this feature.
- Avaya Agent for Desktop shows call appearance which indicates that service observing session is activated and Avaya Agent for Desktop waits for the next call session on observing side.
- Communication Manager then sends the coaching session towards the supervisor.
- Also, Avaya Agent for Desktop uses a binocular icon in place of the incoming/ outgoing calls in the call appearance.
- Avaya Agent for Desktop uses special buttons which allows you to change the SO mode (listen-only, listen-talk, coaching).
- Initially an SO session is in listen-only mode. The supervisor can change this mode to listen-talk during an SO session by pressing the special button on call appearance.
- The supervisor can change the mode to coaching during an SO session by pressing the special button on call appearance (only SIP, if coaching mode available for station).
- The supervisor can stay during the entire call, change mode, or hang-up the call.
- After the call ends, the system goes back to the normal state as a regular station.
- In H.323, it is recommended to stay in an AUX state before a service observing feature activation.

Enabling the supervisor feature from the main screen input box

About this task

There are two flows to enable this feature. In this flow, the coach can supervise agents/VDNs that are not there in the contact database. The agent must add the agent/VDN in the main screen input box and perform the following actions to enable the supervisor feature.

Before you begin

For H.323:, ensure that station or agent is logged in. For SIP, ensure that agent is logged in and must be in an AUX state.

Procedure

1. Type the agent id/VDN in the main screen input box.
2. Click on the drop-down list on the main screen to select **observe** and press Enter.

Note:

- Avaya Agent for Desktop uses the feature button FAC in the background to activate this feature.
- Avaya Agent for Desktop shows call appearance which indicates that service observing session is activated and Avaya Agent for Desktop waits for the next call session on observing side.
- Communication Manager then sends the coaching session towards the supervisor.
- Also, Avaya Agent for Desktop uses a binocular icon in place of the incoming/ outgoing calls in the call appearance.
- Avaya Agent for Desktop uses special buttons which allows you to change the SO mode (listen-only, listen-talk, coaching).
- Initially an SO session is in listen-only mode. The supervisor can change this mode to listen-talk during an SO session by pressing the special button on call appearance.
- The supervisor can change the mode to coaching during an SO session by pressing the special button on call appearance (only SIP, if coaching mode available for station).
- The supervisor can stay during the entire call, change mode, or hang-up the call.
- After the call ends, the system goes back to the normal state as a regular station.
- In H.323, it is recommended to stay in an AUX state before a service observing feature activation.
- You can now activate service observing feature in the Other Phone mode.

Message waiting indicator overview

The Avaya Agent for Desktop system displays a message waiting indicator in the top bar of the main window. When a new voice mail arrives, the message waiting indicator button turns red. When you click the indicator, the system starts a new call to the voice mail number. For using message waiting indicator feature, you must define the user and the mailbox details in Avaya Aura® Messaging. You must also the configure message waiting indicator settings in the Settings window.

Adding a user in Avaya Aura® Messaging

Procedure

1. Log in to the Avaya Aura® Messaging web interface as an administrator.
2. On the **Administration** menu, click **Messaging** > **Messaging System (Storage)** > **User Management**.

The system displays the User Management page.

3. In the **Add a new user** area, click **Add**.

   The system displays the User Properties page.

4. The following fields are mandatory:
   a. **First name**
   b. **Last name**
   c. **Mailbox number**
   d. **Extension**
   e. **New password**
   f. **Confirm password**
5. Click **Save**.

Configuring the message waiting indicator settings

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Preferences** menu.
2. In the **Message Waiting Indicator** area, select the **Show Message Waiting Indicator** check box to activate the message waiting indicator.
3. In the **Voice Mailbox Number** field, enter the appropriate voice mailbox number of the agent.

   Note:

   You must select a DTMF type for the SIP stations only. For H.323, DTMF type is not required.

4. In the **DTMF type** field, click **rtp-payload**.
5. Click **Save**.

Configuring the startup message

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Preferences** menu.
2. In the **Startup Message** field, enter the disclaimer message to display when Avaya Agent for Desktop starts.
3. Click **Save**.

Dialing Rules menu field descriptions

Dialing Rules

Name	Description
Enable dialing rules	The field to activate the dialing rules settings.
Internal Extension Length	The field to specify the length of the internal extension calls. For example, if your internal extensions consist of five digits, enter 5. When you assign the length of the internal extension number, Avaya Agent for Desktop handles the dialed number consisting of the selected number of digits as an internal extension. In the Avaya Agent for Desktop application, you can also add multiple values for **Internal Extension Length** using comma separators.
Local Calling Area Codes	The field to specify the area or city code of Avaya Aura® Communication Manager. For example, 785.
Length of National Phone Numbers	The field to configure the length of national long distance numbers. For example, 10 for North America. In the Avaya Agent for Desktop application, you can also add multiple values for **Length of National Phone Numbers** using comma separators.
Number to Dial to Access External Numbers	The field to specify the number to gain access to an outside line. For example, if you are in North America, you must enter the number as 9 to gain access to the outside line.
Number To Dial For International Calls	The field to specify the international prefix. For example, in North America, type 011.
Number To Dial For Long Distance Calls	The field to specify the national long distance prefix. For example, in North America, type 1.

Table continues…

Name	Description
Your Country Code	The field to specify the country code for Avaya Aura® Communication Manager. For example: 1 for North America, 44 for Great Britain, or 61 for Australia.

Browser Extension Settings

Name	Description
Use Only User Regular Expression	A field to specify that only user`s regular expression will be used for numbers validation.
Regular Expression	A field to define your own regular expression for validation of the numbers. Validation of a specific number occurs in accordance with the country code. A user can configure country code and their own regular expression for validation of numbers. When the user clicks on the number, Avaya Agent for Desktop initiates a new call according to the dialing rules.

Configuring the dialing rules

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

About this task

Dialing rules depend on the country and location of Avaya Aura® Communication Manager. The dialing rules help the system to distinguish extensions from trunk calls, based on the length of the dialing string. Dialing rules ensure that the system uses the right Automatic Route Selection (ARS) code, and if needed, modifies it the digits in with Avaya Aura® Communication Manager, and the PSTN requirements.

Tip:

For traveling agents who go to a different location and need to register with a different Avaya Aura® Communication Manager, you must define the user profile with appropriate dialing rules for the corresponding location and use the login with the corresponding profile so that the dialing rules for the system do not change.

Note:

You must change the dialing rules each time you register the telephone settings with a different Avaya Aura® Communication Manager.

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Dialing Rules** menu.

2. In the **Dialing Rules** section, do the following:
    a. In the **Internal extension length** field, specify the length of the internal extension calls.

        Note:

        Avaya Agent for Desktop supports multiple values for **Internal Extension Length**

    b. In the **Local calling area codes** field, specify the area or city code of Avaya Aura® Communication Manager.
    c. In the **Length of national phone numbers** field, configure the length of national long distance numbers.

        Note:

        Avaya Agent for Desktop supports multiple values for **Length of National Phone Numbers**.

    d. In the **Number to dial to access an external line** field, specify the number to gain access to an outside line. For example, if you are in North America, you must enter the number as 9 to gain access to the outside line.
    e. In the **Number to dial for long distance calls** field, specify the national long distance prefix. For example, in North America, type 1.
    f. In the **Number to dial for international calls** field, specify the international prefix. For example, in North America, type 011.
    g. In the **Your country code** field, specify the country code for Avaya Aura® Communication Manager. For example: 1 for North America, 44 for Great Britain, or 61 for Australia.
3. In the **Browser Extension Settings** section, do the following:
    a. To use the user defined regular expression, select the **Use only user regular expression** check box.
    b. To define the regular expression, in the **User expression** field, type the expression..
4. Click **Save**.

Activating the dialing rules settings

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Dialing Rules** screen.
2. In the **Dialing Rules** section, select the **Enable dialing rules** check box to activate the dialing rules settings.
3. Click **Save**.

4. Restart the Avaya Agent for Desktop application.

Directory menu field descriptions

Directory Settings:

Important:

If you make any changes in the Settings window, you must restart the Avaya Agent for Desktop application.

Name	Supported signalling	Description
Directory Address	Both H.323 and SIP	The field to specify the network domain or the IP address of the public directory server.
Directory Port	Both H.323 and SIP	The field to specify the port of the public directory server.
Directory Root Search	Both H.323 and SIP	The field to enter an LDAP format string representing an information type. For example, `ou=people, o=mycompany.com` specifies that information under the organization unit of people within the organization of *mycompany.com* is used for the search. For information on Base DN or Search Root strings, see the documentation for your LDAP system and the company database configuration.
Directory Username	Both H.323 and SIP	The field to configure the user name to connect to the public directory server. You must provide a user name only if the public directory server requires authorization.
Directory Password	Both H.323 and SIP	The field to enter the password of the user specified in the **Directory username** field.
Save Directory Password	Both H.323 and SIP	The field to allow to save the directory password.

Table continues…

Name	Supported signalling	Description
Bind option	Both H.323 and SIP	The field to choose the LDAP service type. Select one of the following values: • **Simple**: Select this option for using the directory service with an LDAPv2 server. • **GSS bind**: Select this option for using the directory service with an LDAPv3 server. Apple and Linux servers do not support the GSS bind option.

Audio menu field descriptions

Audio Output:

Name	Description
Device	A drop-down list box that contains the audio devices installed on the workstation.
Volume	A slider that controls the volume of the selected output device.
Test	A button for verifying that the selected output device works properly.

Ringer Output:

Name	Description
Device	A drop—down list box that contains the audio devices installed on the workstation.
Volume	A slider that controls the volume of the selected output device.
Test	A button for verifying that the selected output device works properly.

Audio Input:

Name	Description
Device	A drop—down list box that contains the audio devices installed on the workstation.

Table continues…

Name	Description
Volume	A slider that controls the volume of the selected output device.
Test	A button for verifying that the selected output device works properly.
Gain	A field to display the audio volume strength when you test the audio input.

Audio Advance Settings:

Name	Description
Control Device	A field to select the available headset options.

Table continues…

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Headset Integration</td><td>A field to integrate or disintegrate headset capability while it is connected to the desktop application carrying system. The available options are:
Disabled
Basic
Advanced
Note:
The following table provides the list of headsets which cannot answer the very first incoming calls after the headset is connected. It is a known issue and will be resolved in the subsequent releases.<table><tr><th>Head Set List</th><th>Thinpro 64-bit (Debian)</th><th>Igel (linux)</th></tr><tr><td>Plantronics C520</td><td>Voice</td><td>Voice</td></tr><tr><td>Plantronics DA80</td><td>Full</td><td>Full</td></tr><tr><td>Plantronics 300DA</td><td>Full</td><td>Full</td></tr><tr><td>Plantronics 628 USB</td><td>Voice</td><td>Voice</td></tr><tr><td>Plantronics C510</td><td>Voice</td><td>Voice</td></tr><tr><td>Jabra Link 220</td><td>Voice</td><td>Voice</td></tr><tr><td>Jabra Link 280</td><td>Voice</td><td>Voice</td></tr><tr><td>Plantronics C510 M</td><td>Voice</td><td>Voice</td></tr></table></td></tr>
<tr><td>Call Button</td><td>Defines the call controls options for headset call button. Use the following options:
Disabled
Answer
Hold
Drop</td></tr>
</table>

Table continues…

Name	Description
Noise Suppression	Suppresses any possible noise in a call. Use the following options: • **Disabled**: Deactivates the noise suppression. • **Conference**: Noise suppression in a conference call. • **Low**: Low-level noise suppression in a one-to-one call. • **Moderate**: Moderate level noise suppression in a one-to-one call. • **High**: High-level noise suppression in a one-to-one call. • **Very High**: Higher than the high-level noise suppression in a one-to-one call.
Auto Gain Control	Automatically controls the audio volume of a call.
Echo Cancellation	Suppresses any possible echo in a call.

Note:

The **Enable iTunes Playback control** option will be available only for Mac version.

Configuring the audio input

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

Procedure

1. In the Avaya Agent for Desktop Settings window > **Settings** tab, click the **Audio** menu.
2. In the Audio Input area, select the audio device and the volume.
3. (Optional) Click **Test** to test the input device.
4. Click **Save**.

Configuring the audio output

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, select the **Audio** menu.
2. In the Audio Output field, select the audio device and the volume.
3. To test the audio device, click **Test**.
4. Click **Save**.

Configuring the ringer output

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

About this task

By configuring the ringer output, you can select the device that plays the ringing sound when you have an incoming call.

Procedure

1. In the Avaya Agent for DesktopSettings window, on the **Settings** tab, select the **Audio** menu.
2. In the **Ringer Output** area, select the output device and the volume.
3. (Optional) Click **Test** to test the device.
4. Click **Save**.

Configuring the advanced audio settings

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

About this task

By configuring the advanced audio settings, you can suppress echo and noise, and automatically control audio volume.

Procedure

1. In the Avaya Agent for DesktopSettings window, on the **Settings** tab, select the **Audio** menu.
2. To control the Avaya Agent for Desktop calls using a headset, select **Basic** or **Advanced** option from the **Headset Integration** drop-down list.

Note:

If the **Advanced** mode is selected, then the **Call Button** configuration is not available. The **Advanced** mode is applicable only for the Jabra and the Plantronics headsets which have SDK support by vendor. The behavior of the buttons are described in the respective headset user manuals.

3. In the **Control Device** drop-down list, select the available headset option.
4. From the **Call Button** drop-down list, select the desired action you want to use for the headset call button from the following list:
   - **Disabled**
   - **Answer**
   - **Hold**
   - **Drop**
5. In the **Noise Suppression** field, click one of the following options to suppress noise in a call:
   - **Disabled**
   - **Conference**
   - **Low**
   - **Moderate**
   - **High**
   - **Very High**
6. Select the **Auto Gain Control** check box to automatically control the audio volume of a call.
7. Select the **Echo Cancellation** check box to suppress any possible echo in a call.
8. Click **Save**.

Advanced tab field descriptions

Language section

Name	Description
Language	Avaya Agent for Desktop user interface can be viewed in the following languages: **Note:** Avaya Agent for Desktop does not supports information received from Avaya Aura®Communication Manager or any other external components in a language other than English. • English - United States. This is the default language of the Avaya Agent for Desktop user interface. • German - Germany • Spanish - Spain • French - Canada • French - France • Korean - Republic of Korea • Portuguese - Brazil • Russian - Russian Federation • Chinese - China • Arabic - Saudi Arabia • Italian - Italy • Japanese - Japan

Logging section

Name	Description
Log Directory	The user defined storage location for the call logs.
Log Level	The detail level of the log events written by Avaya Agent for Desktop. Choose one of the following values: • **Error** • **Info** • **Debug**

Table continues…

Name	Description
Maximum log files size (in MB)	Use this option to set the log files storage limits. The minimum file size allowed is 5 MB. The maximum file size allowed is 500 MB. If the file size exceeds the maximum limit, the system overrides the older log files.
Include Media Logs	When the **Include media quality logs** check box is selected, media quality logs are included in the remote logs. **Note:** You must select the **Include media quality logs** check box to view **RTCP Monitoring Server Settings** section in the **Advanced** tab.
Enable Remote Logging	When the **Enable Remote Logging** check box is selected, Avaya Agent for Desktop writes event logs on a server other than the machine that runs Avaya Agent for Desktop. This is useful for collecting logs from agents who are experiencing problems with Avaya Agent for Desktop. Avaya Agent for Desktop supports any server that implements standard Syslog messages. When the *Enable Remote Logging* option is enabled, Avaya Agent for Desktop sends UDP packets to the Syslog server through port 514. To reduce the network traffic and the server load, Avaya recommends that you disable remote logging when remote logging is not mandatory.
Remote Logging Server	The remote host IP address for central logging.
Remote Log Level	The detail level for the log events written on the remote server. The available options are: • **Error** • **Info** • **Debug** **Note:** If any problem occurs while running the Avaya Agent for Desktop application, you must set the log level as **Debug** mode. The debug mode option helps in better troubleshooting of the problem.

Note:

Now, you can also save the logs in a zip format on your desktop.

Avaya Agent for Desktop now stores agents' session details in a separate session log file. The session log file is created when the agent logs in to Avaya Agent for Desktop. The system removes the session log file as soon as the agent logs out of the Avaya Agent for Desktop application. The application also stores separate SIP message log files. This log file is created only when the Avaya Agent for Desktop is in Debug log mode.

Quality of Service Tagging section

Name	Description
Use local QoS Settings	Override the QoS settings of Avaya Aura® Communication Manager and Avaya Aura® Session Manager and use the local QoS settings.
Tag DSCP for Audio	Use the local audio DSCP value. This option can be selected only if the **Use local QoS Settings** option is active. After selecting this check box, in the box, type the required value. **Note:** Recommended value is `46` (Expedited Forwarding).
Audio 802.1 p	Use the local audio 802.1 p value. This option can be selected only if the **Use local QoS Settings** option is active. After selecting this check box, in the box, type the required value.
Signalling DSCP	Use the local signalling DSCP value. This option can be selected only if the **Use local QoS Settings** option is active. After selecting this check box, in the box, type the required value. **Note:** For more information on the Signalling DSCP values, see the `Commonly used signalling DSCP values` section.
Signalling 802.1 p	Use the local signalling 802.1 p value. This option can be selected only if the **Use local QoS Settings** option is active. After selecting this check box, in the box, type the required value.

RTCP Monitoring

Name	Description
Server Address	A field to define the IP address of the RTCP server.
Server Port	A field to define the port number of the RTCP server.
Monitoring Period	A field to define the report upload period per second.

Presence

Name	Description
Enable Presence	A field to activate Presence service for the Avaya Agent for Desktop application.

Setting the language for Avaya Agent for Desktop

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

About this task

The Avaya Agent for Desktop user interface is designed for being used in multiple languages.

This procedure describes how to change the language of the Avaya Agent for Desktop user interface.

Procedure

1. In the Avaya Agent for Desktop Configuration window, click the **Advanced** tab.
2. In the **Language** field, click one of the available languages.
3. Click **Save**.

Configuring logs

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

About this task

Log levels indicate the amount of detail that an application uses to write log files.

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Advanced** menu.
2. In the **Log Directory** field, specify the location to store the call logs.
3. In the **Log Level** field, select one of the following values:
   - **Error**
   - **Info**
   - **Debug**

4. (Optional) Select the **Enable Remote Logging** check box to enable logging on a remote server.

   If you enable remote logging, you must also configure the IP address of the remote server and a log level.

   Avaya Agent for Desktop supports any server that implements standard Syslog messages.

   When the *Enable Remote Logging* option is enabled, Avaya Agent for Desktop sends UDP packets to the Syslog server through port 514. To reduce the network traffic and the server load, Avaya recommends that you disable remote logging when remote logging is not mandatory.
5. In the **Maximum log files size** field, specify the maximum file storage space for the log files in MB.
6. (Optional) Select the **Include Media Quality Logs** check box to include media quality information in the Avaya Agent for Desktop logs.
7. Click **Save**.

Configuring the RTCP Monitoring Server settings

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

About this task

Configure the RTCP Monitoring server to store network logs on the RTCP server.

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Advanced** menu.
2. In the **RTCP Monitoring** section, perform the following actions:
   a. In the **Server Address** field, type the IP address of the RTCP server.
   b. In the **Server Port** field, type the port number of the RTCP server.
   c. In the **Monitoring Period** field, type the report upload period per second.
3. Click **Save**.

Configuring QoS tagging for audio

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

About this task

The local QoS settings overrides QoS settings defined in Avaya Aura® Communication Manager and Avaya Aura® Session Manager. You can also enable Differentiated Services Code Point (DSCP) or 802.1 p settings to better manage QoS of the network.

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Advanced** menu.
2. In the **Quality of Service Tagging** section, perform the following actions:
   a. Select the **Use local QoS settings** check box to override the QoS settings of Avaya Aura® Communication Manager and Avaya Aura® Session Manager and use the local QoS settings.
   b. Select the **Audio DSCP** check box and type the required Audio DSCP value.
   c. Select the **Audio 802.1 p** check box and type the required Audio 802.1 p value.

      Note:

      In case you are using Local QoS configuration, you must disable the Audio 802.1 p value.
3. Click **Save**.

Configuring QoS tagging for signals

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

About this task

The local QoS settings for signals overrides QoS settings defined in Avaya Aura® Communication Manager and Avaya Aura® Session Manager. You can also enable Differentiated Services Code Point (DSCP) or 802.1 p settings to better manage QoS of the signals.

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Advanced** menu.
2. In the **Quality of Service Tagging** section, perform the following actions:
   a. Select the **Use local QoS settings** check box to override the QoS settings of Avaya Aura® Communication Manager and Avaya Aura® Session Manager and use the local QoS settings.
   b. Select the **Tag DSCP for Signalling** check box and type the required **DSCP Value for Signalling**.

For more information on DSCP values, see `Commonly used signalling DSCP values`.

c. Select the **Tag 802.1 p for Signalling** check box and type the required **802.1 p Value for Signalling**.

Note:

H.323 implementation of DSCP tagging has following limitations: First UDP signaling message (for example –. first RAS message) from Agent will not be tagged (will be tagged with 0 value) and also first TCP signaling message (for example – first CS message) from Agent will not be tagged. Additionally, in case you are using Local QoS configuration, you must disable the Signalling 802.1 p value.

3. Click **Save**.

Setting failed session removal time

About this task

You can define a failed session time out to limit the time a call rings to an invalid extension.

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Advanced** menu.
2. In the **Session Manager** section on the right pane, in the **Failed Session Removal Timeout** field, specify the desired time in seconds.

Note:

Avaya recommends to set Failed Session Removal Timeout to one second.

3. Click **Save**.
4. Restart the Avaya Agent for Desktop application.

Enabling local media shuffling

About this task

You can enable local media shuffling when direct media is enabled on the telecommuter side and on endpoint side.

Shuffling is done by rerouting the voice channel away from the usual TDM bus connection and creating a direct IP-to-IP connection. Avaya Aura® Communication Manager is used to shuffle call path connections between IP endpoints.

Before you begin

Ensure that the **Login mode** field is set as **Other Phone** mode on the **Preferences** menu on the **Settings** window.

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Advanced** menu.
2. In the **Session Manager** section on the right pane, select the **Enable Local Media Shuffling** check box.
3. Click **Save**.
4. Restart the Avaya Agent for Desktop application.

Deleting the log files manually

About this task

As part of the data protection procedure, you can delete the Avaya Agent for Desktop log files manually.

Before you begin

- Ensure that you have administrator rights on the system from which you are going to manually delete the log files.
- You must exit the Avaya Agent for Desktop application before deleting the log files.

Procedure

1. In the Avaya Agent for Desktop **Settings** window, on the **Settings** tab, click the **Advanced** menu.
2. Navigate to the system path defined in the **Log Directory** field and manually delete the log files.

Security menu field descriptions

Password Storage

Name	Description
Password storage mode	A field to allow a password to load from the specified storage option. The options are: • **Security Storage Only**: Loads password from a secured storage only. • **Security Storage If Available**: Loads password from a secured storage if available otherwise loads from a non-secure storage. • **Non-secure Storage Only**: Loads password from a non-secure storage only.

PPM Secure Mode section

Name	Description
HTTP	The unsecured way to connect to the servers on the World Wide Web.
HTTPS	The secured and encrypted way to connect to the servers on the World Wide Web.

Third-Party Certification section

Avaya Agent for Desktop can be configured to use TLS (Transport Layer Security) when connecting to the SIP proxy. TLS implementation involves digital certificate exchange for securing the communication. A non-unique, default TLS certificates, certified by Avaya, are shipped with Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager, and Avaya one-X® Deskphone SIP to provide required support for TLS sessions.

For production environments, you must replace the default certificates with customer CA or third-party CA signed unique identity certificates.

Name	Description
Not Used	The option to disable the third-party certification authentication.

Table continues…

Name	Description
Use Local	The option to select the third-party certificate installed on your local system. When you select this option, the system displays the **Certificates** field. Click the ⊕ icon to select the certificate from your local system. **Note:** If you have installed a Trusted Third-Party (TTP) certificate on your local drive, you must import the installed certificate from the local drive to the **certs** folder of Avaya Agent for Desktop so that it can use the same certificate.
Remote	The option to select the third-party certificate located on a remote server. When you select this option, the system displays the **Certificates Remote Host** field. In the **Certificates Remote Host** field, you can choose to select the certificate from an **HTTP** or an **HTTPS** location. You must provide the **Remote Address** and the **Remote Port** number of the remote server for all cases. For an **HTTP** location, provide 80 as a port number. For an **HTTPS** location, provide 443 as a port number. You must also modify and add the following line in the **96x1Supgrade.txt** file on the remote server: `SET TRUSTCERTS cert.pem` **Note:** **cert.pem** and **96x1Supgrade.txt** files must be in the same folder.

Identity certification section

Avaya Agent for Desktop can be configured to use TLS (Transport Layer Security) mutual authentication when connecting to the SIP proxy. TLS mutual authentication mode requires both the server endpoint and client endpoint to exchange X.509 certificates for authentication. Avaya Agent for Desktop provides ability to setup client identity certificate.

Avaya Agent for Desktop supports the four options to install client identity certificate as shown in the following table:

Name	Description
Not used	The option to disable the identity certification authentication. In this case, Avaya Agent for Desktop uses embedded Avaya certificate. **Important:** It is highly recommended that customer's must use their certificate in any case.
Use Local	The option to select the identity certificate installed on your local system. When you select this option, **Certificate Path**, **Certificate Password**, and **Save Certificate Password** fields are displayed. In this case, browse and locate local PKCS12 certificate file. X.509 certificate and private key will be extracted from this file. You also need to provide the password to access this file. You can also choose to save this password.
Remote	The option to select the identity certificate located on a remote server. When you select this option, **Certificate Path**, **Certificate Password**, and **Save Certificate Password** fields are displayed. In this case, browse and locate remote PKCS12 certificate file. X.509 certificate and private key will be extracted from this file. You also need to provide the password to access this file. You must also modify and add the URL to certificate with certificate name in the **96x1Supgrade.txt** file on the remote server: `SET PKCS12URL http://<Server IP address>/userCertificate.p12`

Table continues…

Name	Description
Certificate Authority	The option to request X.509 certificate using Simple Certificate Enrollment Protocol (SCEP) from Certificate Authority server. In case when Avaya Agent for Desktop is unable to get the certificate, previously downloaded certificate will be used. If this certificate does not exist, embedded Avaya certificate will be used. The options to configure this settings are: • **Certificate Password**: This value is used to store the certificate from the Certificate Authority server. This value will replace *$PASSWD* variable. • **Save Certificate Password**: The option to save the password provided for the Certificate. • **Certificate Authority URL**: Specify the URL of the SCEP server from which the Avaya Agent for Desktop must obtain an identity certificates. Only HTTP protocol is currently supported. • **Certificate Authority Password**: This value is used to specify the password to be included (if not null) in the challengePassword attribute of an SCEP certificate request. It can be specified only through using variables *$MACADDR* or *$PASSWD*. If the value contains *$PASSWD*, it will be replaced by the value from Password field. If the value contains *$MACADDR*, it will be replaced by the machine's MAC address in hex. • **Common Name**: Specify the Common Name (CN) used in the SUBJECT of an SCEP certificate request. The value must be a string that contains either *$PASSWD* (this will be replaced by the value from Password field) or *$MACADDR* (this will be replaced by the machine's MAC address). • **Distinguished name**: This value is part of the SUBJECT of an SCEP certificate request. It must begin with `/` and may include Organizational Unit, Organization, Location, State, and Country. For example: `/DC=COM/DC=Avaya`. • **Key Length**: Specify the bit length of the public and private keys that will generated for the SCEP certificate request. The default value is 1024.

SRTP section

Name	Description
Enable SRTP	The option to activate Secure Real-Time Transport Protocol (SRTP) encryption method.
Media Encryption Parameters	The option to provide parameter value for various methods of using SRTP. You must configure the Avaya Communication Manager (CM) SRTP settings as per the values provided in this field. For example, you can use any of the following values as parameter: • 9 — This is a default value which means none or disabled SRTP or RTP. • 1, 9 — Use this SRTP value to activate fall back on RTP encryption in case of failure. • 2, 9 — Use this SRTP value to allow fall back on RTP encryption in case of failure. • 1, 2, 9 — Use this SRTP value to allow fall back on RTP encryption in case of failure. **Note:** There are total nine (1–9) SRTP media encryption parameter available. In case of CM 6.3, three levels of encryptions are supported. In case of CM 7.0, five levels of encryptions are supported. In case of Avaya Agent for Desktop, only three levels — 1, 2, 9 are supported.
Enable SRTCP	The option to activate Secure Real Time Control Protocol (SRTCP) encryption method. SRTCP allows you to securely send media statistics from Avaya Agent for Desktop.

Extended Validation

Name	Description
Hostname Validation	A field to activate and define hostname validation types: The available options are: • **Disabled** • **Informational** • **Enforced**

Table continues…

Name	Description
Domain Validation	A field to activate and define domain validation types: The available options are: • **Disabled** • **Informational** • **Enforced**

Internal Browser

Name	Description
Ignore all SSL Errors in Browser	A field to suppress the SSL error notifications popping from the internal browser.

ACM

Name	Description
Ignore SSL Errors from ACM	A field to suppress the SSL error notifications popping from ACM.

Changing the user password using Config.xml file

You can now change the Avaya Agent for Desktop's local user password using Config.xml. To use password from Config.xml file and not from Security Storage, you need to activate the UsePSWDFromConfigFile parameter in the Config.xml file. By default this parameter is set to false and must be changed to true. When this parameter is enabled, Avaya Agent for Desktop reads password from Config.xml and not from Security Storage.

Configuring the PPM Secure Mode settings

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

About this task

Modes for secured Personal Profile Management (PPM) for SIP.

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Security** menu.
2. In the **PPM Secure Mode** section, click one of the following options:
   - **HTTP**

- **HTTPS**

3. Click **Save**.

Configuring the third-party certificate security settings

About this task

Use the following procedure to apply a certificate so that the system can establish a secured connection with Avaya Aura® Session Manager or Session Border Controller (SBC).

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Security** menu.
2. In the **Third-party Certification** section, click one of the following options:
   - **Not Used**: Click this option to disable the third-party certificate authentication.
   - **Use Local**: Click this option to select the third-party certificate from the local system.
   - **Remote**: Click this option to select the third-party certificate from the remote server. You must provide the required **Remote Address** and **Remote Port** number of the remote server.

     Note:

     For an **HTTP** location, provide 80 as a port number. For an **HTTPS** location, provide 443 as a port number.

     You must also modify and add the following line in the **96x1Supgrade.txt** file on the remote server:

     ```
     SET TRUSTCERTS cert.pem
     ```

     Note:

     cert.pem and **96x1Supgrade.txt** files must be in the same folder.
3. Click **Save**.
4. Restart the Avaya Agent for Desktop application.

Configuring the SRTP and SRTCP settings

Procedure

1. In the Avaya Agent for DesktopSettings window, on the **Settings** tab, click the **Security** menu.
2. In the **SRTP** section, do the following:
   - Select the **Enable SRTP** check box to activate the SRTP settings.

- Select the **Enable SRTCP** check box to activate the SRTCP settings.

  Note:

  - SRTCP is not enabled by default. You must select the **Enable SRTCP** check box to enable SRTP.
  - SRTCP will only be used if it is also configured on Avaya Aura® Communication Manager.

3. In the **Media Encryption Parameters** field, type the required parameter value.

   Note:

   You must configure the Avaya Communication Manager SRTP and SRTCP settings as per the values provided in this field.

4. Click **Save**.
5. Restart the Avaya Agent for Desktop application.

Avaya Agent for Desktop Presence feature overview

About Presence feature

Avaya Agent for Desktop now supports Avaya Presence feature. Using Presence feature, an agent can publish their presence details, such as availability, on-phone state, notes, and also observe presence of another agent. Avaya Agent for Desktop enhances the standard Avaya Presence states by correlating them to the standard agent states, such as AUX, ACW, Ready, etc., with the additional presence note. Presence works in a shared control mode only if Avaya Agent for Desktop is used on both side (Controlled and controlling). This feature works only if you are using SIP protocol.

Note:

Presence is unavailable if you connect Avaya Agent for Desktop using H.323.

Presence starts on its own when the station is logged in. A user does not need to make any configuration for presence server as these settings are received in Avaya Agent for Desktopvia PPM. A user must enable the Presence feature though in the **Settings** window.

The presence feature displays both agent's presence and presence of contacts in the agent's contact list.

About Self Presence

- Whenever user logs in on a station, Presence shows offline state.
- Whenever user logs in on agent extension, Avaya Agent for Desktop Presence shows away state.
- Whenever an agent changes its state, Avaya Agent for Desktop Presence changes according to agent state.
- Whenever an agent changes state to **Do not disturb**, the Presence shows Do not disturb. From Agent point of view, **Do not disturb** is an Aux agent state with specific reason code.

- Whenever an agent logs out or application is closed, Presence shows offline state.

Table 11:

Main window icon	Agent State tooltip	Presence	Presence Note
	Ready	Available	-
	Ready (on a Call)	On a phone	On a call
	Ready (on a Call)	On a phone	ACD call
	Aux	Away	A reason code description
	After Call Work	Busy	After Call work
	Do not disturb	Do not disturb	Do not disturb
	Offline	Offline	-

Presence for Station and Agent

If you choose the presence type as **Enable Presence for Station and Agent**, then there are two additional states. If an agent is signed in all other states except the offline state, then Avaya Agent for Desktop works the same as for **Enable Presence for Agent Only** presence type.

Table 12:

Main window icon	Agent state tooltip	Presence	Comments
	Station State: Available, Agent State: Offline	Available	Only station is signed-in. Agent state is offline. There are no active calls.
	Station State: Busy, Agent State: Offline	On a phone	Only station is signed-in. Agent state is offline. There is an active call.

About Contact list Presence

- An agent can view the Presence of agents for whom Presence is configured and active. Both the agents must be in the same domain as observer.
- Key value is work phone. Avaya Agent for Desktop uses work number as base of subscription address.
- A column in the Contact list represents a Contact list Presence with tool tip. A tool tip is a presence note.
- If a contact is added during an active agent work session, Presence initially shows offline. But after sometime, the status is updated.

Table 13:

Contact icon	Contact Agent state	Contact Presence	Contact Presence tool tip
	Ready	Available	-
	Ready (on a call)	On a phone	On a call
	Ready (on a call)	On a phone	ACD call
	Aux	Away	Aux : with aux description
	After Call Work	Busy	After Call Work
	Aux	Do not disturb	Do not disturb
	Offline	Offline	
	Unknown	Unknown	

Note:

Following are some limitations of Presence feature:

- Presence for LDAP search does not work.
- Presence is currently supported for SIP signaling only.
- Presence is not reset to offline mode when failover occurs.

Activating the Presence feature settings

About this task

You must be sure that Avaya Agent for Desktop is using TLS connection. To activate this feature, your administrator must enable the Presence option in your Avaya Agent for Desktop **Settings** and configure SIP endpoint for Presence Services

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Advanced** menu.
2. In the **Presence** section, select the **Enable Presence** check box to activate the Presence settings.
3. Click **Save**.
4. Restart the Avaya Agent for Desktop application.

Commonly used Signalling DSCP values

DSCP value	Hex value	Decimal value	Meaning	Drop probability	Equivalent IP precedence value
101 110	0x2e	46	Expedited forwarding (EF)	N/A	101 – Critical
000 000	0x00	0	Best effort	N/A	000 – Routine
001 010	0x0a	10	AF11	Low	001 – Priority
001 100	0x0c	12	AF12	Medium	001 – Priority
001 110	0x0e	14	AF13	High	001 – Priority
010 010	0x12	18	AF21	Low	010 – Immediate
010 100	0x14	20	AF22	Medium	010 – Immediate
010 110	0x16	22	AF23	High	010 – Immediate
011 010	0x1a	26	AF31	Low	011 – Flash
011 100	0x1c	28	AF32	Medium	011 – Flash
011 110	0x1e	30	AF33	High	011 – Flash
100 010	0x22	34	AF41	Low	100 – Flash override
100 100	0x24	36	AF42	Medium	100 – Flash override
100 110	0x26	38	AF43	High	100 – Flash override

Disabling SSL error notifications

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Security** menu.
2. In the **Internal Browser** section, clear the **Ignore All SSL Errors in Browser** check box to suppress the SSL error notifications popping from the internal browsers.
3. In the **ACM** section, clear the **Ignore All SSL Errors from ACM** check box to suppress the SSL error notifications popping from ACM.
4. Click **Save**.
5. Restart the Avaya Agent for Desktop application.

Configuring the Identity certificate security settings

About this task

Use the following procedure to apply an identity certificate for mutual authentication. TLS mutual authentication mode requires both the server endpoint and client endpoint to exchange X.509 certificates for authentication.

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Security** menu.
2. In the **Identity Certification** section, click any one of the following **Certificate Mode** options:
   - **Not used**: Click this option to disable the identity certificate authentication.
   - **Use local**: Click this option to select the identity certificate from the local system.
   - **Use remote host**: Click this option to select the identity certificate from the remote server.
   - **Use Certificate Authority**: Click this option to generate the identity certificate through the Simple Certificate Enrollment Protocol (SCEP) server.

   For more details on configuring the identity certificate security settings, see the `Security tab field descriptions` section.
3. Click **Save**.
4. Restart the Avaya Agent for Desktop application.

Configuring the Identity certificate security settings

About this task

Use the following procedure to apply an identity certificate for mutual authentication. TLS mutual authentication mode requires both the server endpoint and client endpoint to exchange X.509 certificates for authentication.

Procedure

1. In the Avaya Agent for Desktop Settings window, on the **Settings** tab, click the **Security** menu.
2. In the **Identity Certification** section, click any one of the following **Certificate Mode** options:
   - **Not used**: Click this option to disable the identity certificate authentication.
   - **Use local**: Click this option to select the identity certificate from the local system.
   - **Use remote host**: Click this option to select the identity certificate from the remote server.

- **Use Certificate Authority**: Click this option to generate the identity certificate through the Simple Certificate Enrollment Protocol (SCEP) server.

For more details on configuring the identity certificate security settings, see the `Security tab field descriptions` section.

3. Click **Save**.
4. Restart the Avaya Agent for Desktop application.

Setting up the network disconnection alert using config.xml file

About this task

- You can setup a network disconnection alert timer parameter in the config.xml file.
- The parameter when with a value of 0 (zero) the network disconnect message will display immediately after a network failure.
- The parameter when with a value of 1 or above will represent how many seconds the application should wait before showing the error message.
- If the network is recovered before the timer, no error message will be shown.
- If the timer expires the error message will be shown.
- A value of 999 means the error message is completely disabled and will never be shown.

Before you begin

Ensure that you have the administrator rights to modify the confiig.xml file.

Procedure

1. Navigate to `C:\Users\<user name>\AppData\Roaming\Avaya\Avaya Agent`.
2. Type details as shown in the following example and save the file.

Example

```
<parameter><name>NetworkErrorNotifyDelay</name><value>10</value></parameter>
```

Lock Manager overview

Avaya Agent for Desktop now provides option prevent a menu or a tab on the **Settings** window from modification. For preventing the **Settings** from modification, you need to update the configuration XML file with the proper name of the UI controls.

The lock manager configuration XML file must be placed into < AVAYA_AGENT_CONFIG_DIR> for any platforms or < AVAYA_AGENT_INSTALL_DIR\share\> folder for Windows and </Contents/Resources/usr/share/avaya-agent/> folder for Mac OS X. The lock manager file should be named as `LockManager.xml`.

Sample Lock Manager XML file

```
<?xml version="1.0" encoding="UTF-8" ?>
<UIFields>
        <disable name="ConfigurationDialog_DialingRulesTab_LocalAreaNumberTextLengthEdit"/>
        <disable name="ConfigurationDialog_PreferencesTab_LoginModeComboBox"/>
        <disable name="ConfigurationDialog_PreferencesTab_TelecommuteNumberLine"/>
        <disable name="ConfigurationDialog_AdvancedTab_LocalQoSSettingsCheckBox"/>
        <disable name="ConfigurationDialog_AudioTab"/>
        <disable name="ConfigurationDialog_PreferencesTab_ShowUICheckBox"/>
<!--    <disable name="ConfigurationDialog_DialingRulesTab_LocalAreaNumberTextLengthEdir"/> -->
<!--    <disable name="ConfigurationDialog_AudioTab"/> -->
        <!--<disable name="ConfigurationDialog_PreferencesTab"/> -->
</UIFields>
```

Lock Manager lock name for UI controls

Login Dialog

UI control placement	UI control name
Station ID	LoginDialog_StationLoginLineEdit
Station Password	LoginDialog_StationPasswordLineEdit
Save password check box for station	LoginDialog_StationSavePasswordCheckBox
Agent ID	LoginDialog_AgentLoginLineEdit
Agent Password	LoginDialog_AgentPasswordLineEdit
Save password (for agent) checkbox	LoginDialog_AgentSavePasswordCheckBox
ACM Account	LoginDialog_ACCCMLoginLineEdit
ACM Password	LoginDialog_ACCCMPasswordLineEdit
Save password (for ACM) checkbox	LoginDialog_ACCCMSavePasswordCheckBox
Automatic Sign In (for agent) checkbox	LoginDialog_AgentAutoLoginCheckBox
Use for audio (login mode)	LoginDialog_LoginModeComboBox
Other Phone Number	LoginDialog_TelecommuteNumberEdit
Settings button	LoginDialog_ConfigBtn
Close button	LoginDialog_CancelBtn
Sign In All button	LoginDialog_LoginBtn
Basic / Advanced button	LoginDialog_BtnBasicAdvanced
Automatic Sign In (for ACM) checkbox	LoginDialog_ACMAutoLoginCheckBox
Automatic Sign In (for station) checkbox	LoginDialog_StationAutoLoginCheckBox
ACM Sign In button	LoginDialog_ACMSignInBtn
ACM Sign Out button	LoginDialog_ACMSignOutBtn

Table continues…

UI control placement	UI control name
Station Sign In button	LoginDialog_StationSignInBtn
Station Sign Out button	LoginDialog_StationSignOutBtn
Agent Sign In button	LoginDialog_AgentSignInBtn
Agent Sign Out button	LoginDialog_AgentSignOutBtn
Profile selection box	LoginDialog_ACMProfileComboBox
Profile confirm button	LoginDialog_SelectProfileBtn

Main window

UI control placement	UI control name
DialPad button	MainWindow_BtnDialPad
History button	MainWindow_BtnHistory
Contacts button	MainWindow_BtnContacts
MWI button	MainWindow_BtnMWI
Browser button	MainWindow_BtnBrowser
Features button	MainWindow_BtnFeatures
Stats Console button	MainWindow_BtnStatsConsole
Media Quality button	MainWindow_BtnMediaQuality
Speaker button (mute - unmute)	MainWindow_BtnSpeaker
Microphone button (mute - unmute) (applicable for My Computer Mode)	MainWindow_BtnMicrophone

Main window drop down menu

UI control placement	UI control name	Applicable for Headless Mode
Station Logout	MainWindow_ActLogout	true
Collapsed Mode	MainWindow_ActCollapsed	
Settings	MainWindow_ActConfiguration	true
Always on Top	MainWindow_ActAlwaysOnTop	
Hide Interface	MainWindow_ActHideInterface	
Reset Window Position	MainWindow_ActResetWindow	
Stats Console	MainWindow_ActStatsConsole	
Mute	MainWindow_ActMute	true
About	MainWindow_ActAbout	true
Logs	MainWindow_ActLogs	true
Logs → Save As	MainWindow_ActLogsSaveAs	true
ACM Login / Register Station	MainWindow_ActRegister	true
ACM Logout	MainWindow_ActACMLogout	true

Table continues…

UI control placement	UI control name	Applicable for Headless Mode
Workspace	MainWindow_ActWorkspace	
Workspace → Load Workspace	MainWindow_LoadWorkspaceMenu	
Workspace → Save Workspace As	MainWindow_SaveWorkspaceMenu	
Workspace → Manage Workspace	MainWindow_ManageWorkspaceMenu	
Workspace → Lock Windows Position	MainWindow_LockWindowsPosition	
Workspace → Load Workspace → “name” (to disable workspace with name “name”)	MainWindow_LoadWorkspaceMenu_ActMenu_name	
Workspace → Save Workspace As →Save Workspace As New	MainWindow_SaveWorkspaceMenu_ActAdd	
Workspace → Save Workspace As → ”name” ” (to disable workspace with name “name”)	MainWindow_SaveWorkspaceMenu_ActMenu_name	
Workspace → Manage Workspace → “name” ” (to disable workspace with name “name”)	MainWindow_ManageWorkspaceMenu_ActMenu_name	
Agent Register	MainWindow_ActAgentRegister	
Ready	MainWindow_ActAgentReady	
After Call Work	MainWindow_ActAgentACW	
Auxiliary	MainWindow_MenuAUX MainWindow_ActAgntAUX	
Auxiliary →reason code "number"	MainWindow_MenuAUX_ActReasonCode_number	
Agent Log Out	MainWindow_MenuLogout MainWindow_ActAgntLogout	
Agent Log Out → reason code "number"	MainWindow_MenuLogout_ActReasonCode_number	

Table 14: Call Panel

UI control placement	UI control name
Transfer button	CallPanel_TransferBtn
Conference button	CallPanel_ConferenceBtn
Init Service Observing button	CallPanel_SOInitBtn
Drop Service Observing Session button	CallPanel_SODropBtn

Table continues…

UI control placement	UI control name
DTMF button	CallPanel_EnableDTMFBtn
Hold Call button	CallPanel_HoldCallBtn
Retrieve Call button	CallPanel_RetrieveCallBtn
Init Call button	CallPanel_InitCallBtn
Accept Call button	CallPanel_AcceptCallBtn
Reject Call button	CallPanel_RejectCallBtn
Join Call button	CallPanel_JoinCallBtn
Complete Transfer button	CallPanel_CompletTransferBtn
Complete Conference	CallPanel_CompleteConferenceBtn
Call Work Code button	CallPanel_CallWorkCodeBtn

Contact List

UI control placement	UI control name
Edit Contact Dialog	ContactListDialog_EditContactDialog
Context menu	ContactListDialog_ContextMenu
Contacts Table	ContactListDialog_ContactTableView
Filter button (All Contacts, Favourite, Speed Dial)	ContactListDialog_BtnFilter
All contacts button	ContactListDialog_BtAll
Add Contact button	ContactListDialog_BtnAddContact
Delete contact button and delete item in context menu	ContactListDialog_BtnDeleteContact
Favorites button	ContactListDialog_BtnFavorites
Speed Dial button	ContactListDialog_BtnSpeedDial
Search text box	ContactListDialog_SearchTextBox

History

UI control placement	UI control name
History Table	HistoryDialog_HistoryTableView
Filter button	HistoryDialog_BtnPeriod
Search text box	HistoryDialog_SearchTextBox

Settings Tab

UI control placement	UI control name	Control Names from 1.7 Release (It can also be used to lock this control)
Settings tab	ConfigurationDialog_SettingsTab	

Table continues…

UI control placement	UI control name	Control Names from 1.7 Release (It can also be used to lock this control)
Avaya Control Manager Settings	ConfigurationDialog_SettingsTab_ACMSettings	
Avaya Control Manager Settings → ACM Login Type	ConfigurationDialog_SettingsTab_ACMSettings_ACMLoginType	ConfigurationDialog_ServerTab_UseLocalConfigCheckBox ConfigurationDialog_ServerTab_TypeOfACMComboBox
Avaya Control Manager Settings → Primary ACM Address URL	ConfigurationDialog_SettingsTab_ACMSettings_PrimaryURL	ConfigurationDialog_ServerTab_PrimaryACCCMAddressLineEdit
Avaya Control Manager Settings → Secondary ACM Address URL	ConfigurationDialog_SettingsTab_ACMSettings_SecondaryURL	ConfigurationDialog_ServerTab_SecondaryACCCMAddressLineEdit
Preferred AADS SAML login type	ConfigurationDialog_SettingsTab_ACMSettings_AADSAMLLoginType ConfigurationDialog_SettingsTab_AADS	
Ignore SSL Errors from AADS	ConfigurationDialog_SettingsTab_AADS_IgnoreAADSErrors	
License Server Settings	ConfigurationDialog_SettingsTab_LicenseSettings	
License Server Settings → License Server URL	ConfigurationDialog_SettingsTab_LicenseSettings_LicenseServer	ConfigurationDialog_ServerTab_LicenseServerUrlLineEdit
Local Server Settings	ConfigurationDialog_SettingsTab_ServerSettings	
Local Server Settings → Signaling	ConfigurationDialog_SettingsTab_ServerSettings_Signaling	ConfigurationDialog_ServerTab_SIPRadioBtn ConfigurationDialog_ServerTab_H323RadioBtn
For SIP only: Local Server Settings → Primary SIP Proxy Address	ConfigurationDialog_SettingsTab_ServerSettings_PrimaryAddress	ConfigurationDialog_ServerTab_PrimaryAddressLineEdit ConfigurationDialog_ServerTab_PrimaryAddressPortLineEdit ConfigurationDialog_ServerTab_PrimaryAddressProtocolComboBox

Table continues…

UI control placement	UI control name	Control Names from 1.7 Release (It can also be used to lock this control)
For SIP only: Local Server Settings → Secondary SIP Proxy Address	ConfigurationDialog_SettingsTab_ServerSettings_SecondaryAddress	ConfigurationDialog_ServerTab_SecondaryAddressLineEdit ConfigurationDialog_ServerTab_SecondaryAddressPortLineEdit ConfigurationDialog_ServerTab_SecondaryAddressProtocolComboBox
For H323 only: Local Server Settings → Primary CM Address	ConfigurationDialog_SettingsTab_ServerSettings_PrimaryCMAddress	
For H323 only: Local Server Settings → Secondary CM Address	ConfigurationDialog_SettingsTab_ServerSettings_SecondaryCMAddress	
Local Server Settings → SIP domain	ConfigurationDialog_SettingsTab_ServerSettings_SIPDomain	ConfigurationDialog_ServerTab_DomainLineEdit
Local Server Settings → Number of Connection Attempts	ConfigurationDialog_SettingsTab_ServerSettings_NumberOfAttempts	ConfigurationDialog_ServerTab_MaxAttemptsLineEdite
Local Server Settings → CM Auto Answer Support Required	ConfigurationDialog_SettingsTab_ServerSetting_CMAutoAnswer	ConfigurationDialog_PreferencesTab_CMAutoAnswerCheckBox
ServerSettings_CMAutoAnswer	ConfigurationDialog_PreferencesTab_CMAutoAnswerCheckBox	
Local Server Settings → CM On-hook Dialing Support Required	ConfigurationDialog_SettingsTab_ServerSettings_CMOnhookDialing	
Local Server Settings → CM Forced type of Aux Reason Code Support Required	ConfigurationDialog_SettingsTab_ServerSettings_CMForcedAux	ConfigurationDialog_PreferencesTab_CMForcedAuxCheckBox
Directory Settings	ConfigurationDialog_SettingsTab_DirectorySettings	
Directory Settings → Directory Address	ConfigurationDialog_SettingsTab_DirectorySettings_DirectoryAddress	ConfigurationDialog_ServerTab_DirectoryAddressLineEdit
Directory Settings → Directory Port	ConfigurationDialog_SettingsTab_DirectorySettings_Port	ConfigurationDialog_ServerTab_DirectoryPortLineEdit
Directory Settings → Directory User Name	ConfigurationDialog_SettingsTab_DirectorySettings_UserName	ConfigurationDialog_ServerTab_DirectoryUserLineEdit
Directory Settings → Directory Password	ConfigurationDialog_SettingsTab_DirectorySettings_Password	ConfigurationDialog_ServerTab_DirectoryPasswordLineEdit

Table continues…

UI control placement	UI control name	Control Names from 1.7 Release (It can also be used to lock this control)
Directory Settings → Save Directory Password	ConfigurationDialog_SettingsTab_DirectorySettings_SavePassword	
Directory Settings → Directory Root Search	ConfigurationDialog_SettingsTab_DirectorySettings_RootSearch	ConfigurationDialog_ServerTab_DirectoryRootLineEdit
Directory Settings → Bind Option	ConfigurationDialog_SettingsTab_DirectorySettings_BindOption	ConfigurationDialog_ServerTab_BindOptionComboBox
Dialing Rules	ConfigurationDialog_SettingsTab_DialingRules	ConfigurationDialog_DialingRulesTab_DialingRulesGroupBox
Dialing Rules → Enable Dialing Rules	ConfigurationDialog_SettingsTab_DialingRules_EnableDialingRules	ConfigurationDialog_DialingRulesTab_EnableDialingRulesCheckBox
Dialing Rules → Internal Extension Length	ConfigurationDialog_SettingsTab_DialingRules_InternalExtentionLength	ConfigurationDialog_DialingRulesTab_InternalExtentionLengthTextEdit
Dialing Rules → Local Calling Area Codes	ConfigurationDialog_SettingsTab_DialingRules_LocalCode	ConfigurationDialog_DialingRulesTab_LocalAreaNumberTextLengthEdit
Dialing Rules → Length of National Phone Numbers	ConfigurationDialog_SettingsTab_DialingRules_NationalNumber	ConfigurationDialog_DialingRulesTab_NationalNumberLengthTextEdit
Dialing Rules → Number To Dial To Access External Numbers	ConfigurationDialog_SettingsTab_DialingRules_ExternalNumbers	ConfigurationDialog_DialingRulesTab_PrefixDigitsToAccessExternalLineTextEdit
Dialing Rules → Number To Dial To International Calls	ConfigurationDialog_SettingsTab_DialingRules_InternationalNumbers	ConfigurationDialog_DialingRulesTab_PrefixDigitsToInternationalTextEdit
Dialing Rules → Number To Dial for Long Distance Calls	ConfigurationDialog_SettingsTab_DialingRules_LongDistanceNumbers	ConfigurationDialog_DialingRulesTab_PrefixDigitsToLongDistanceCallsTextEdit
Dialing Rules → Your Country Code	ConfigurationDialog_SettingsTab_DialingRules_CountryCode	ConfigurationDialog_DialingRulesTab_YourCountryCodeTextEdit
Browser Extension	ConfigurationDialog_SettingsTab_BrowserExtension	
Browser Extension → Use Only User Regular Expression	ConfigurationDialog_SettingsTab_BrowserExtension_OnlyUserRegExp	
Browser Extension → Regular Expression	ConfigurationDialog_SettingsTab_BrowserExtension_RegExp	

Table continues…

UI control placement	UI control name	Control Names from 1.7 Release (It can also be used to lock this control)
Agent Settings	ConfigurationDialog_SettingsTab_Agent	
Agent Settings → Ready Mode	ConfigurationDialog_SettingsTab_Agent_ReadyMode	ConfigurationDialog_PreferencesTab_ReadyModeAutoInRadioBtn ConfigurationDialog_PreferencesTab_ReadyModeManualInRadioBtn
Agent Settings → Timed After Call Work	ConfigurationDialog_SettingsTab_Agent_TimedACW	ConfigurationDialog_PreferencesTab_TimedAcwCheckBox
Agent Settings → After Call Work Duration (seconds)	ConfigurationDialog_SettingsTab_Agent_ACWDuration	ConfigurationDialog_PreferencesTab_TimedAcwInterval ConfigurationDialog_PreferencesTab_TimedAcwIntervalLabel
Agent Settings → Allow Manual After Call Work	ConfigurationDialog_SettingsTab_Agent_AllowManualACW	ConfigurationDialog_PreferencesTab_AllowManualAcwCheckBox
Common	ConfigurationDialog_SettingsTab_Common	
Common → Automatically Login The Agent	ConfigurationDialog_SettingsTab_Common_AutoAgentLogin	ConfigurationDialog_PreferencesTab_AutomaticLoginCheckBox
Common → Launch Avaya Agent When Windows Starts	ConfigurationDialog_SettingsTab_Common_AutoStart	ConfigurationDialog_PreferencesTab_AutoStartCheckBox
Common → Show User Interface	ConfigurationDialog_SettingsTab_Common_ShowUI	ConfigurationDialog_PreferencesTab_ShowUICheckBox
Common → Always Display The Main Window On Top	ConfigurationDialog_SettingsTab_Common_WindowOnTop	ConfigurationDialog_PreferencesTab_AlwaysOnTopCheckBox
Common → Local Auto Answer	ConfigurationDialog_SettingsTab_Common_AutoAnswer	ConfigurationDialog_PreferencesTab_AutoAnswerCheckBox
Common → Stay In Notification Area If Main Window Is Closed	ConfigurationDialog_SettingsTab_Common_StayInTrayButton	ConfigurationDialog_PreferencesTab_StayInTrayCheckBox
Common → Show WebLM Server Warning Messages	ConfigurationDialog_SettingsTab_Common_ShowWebLMNotification	
Common → Permanent Network Error Messages	ConfigurationDialog_SettingsTab_Common_PermanentNetworkErrorMessages	
Default Agent State	ConfigurationDialog_SettingsTab_DefaultAgentState	

Table continues…

UI control placement	UI control name	Control Names from 1.7 Release (It can also be used to lock this control)
Default Agent State → Agent state upon login	ConfigurationDialog_SettingsTab_DefaultAgentState_AgentStateUponLogin	
Default Agent State → Agent state recovery timeout after network outage	ConfigurationDialog_SettingsTab_DefaultAgentState_AgentStateRecoveryTimer	
Login Mode	ConfigurationDialog_SettingsTab_LoginMode	ConfigurationDialog_PreferencesTab_loginModeGroupBox
Login Mode → Login Mode	ConfigurationDialog_SettingsTab_LoginMode_LoginMode	ConfigurationDialog_PreferencesTab_LoginModeComboBox
Login Mode → Other Phone Number	ConfigurationDialog_SettingsTab_LoginMode_TCNumber	ConfigurationDialog_PreferencesTab_TelecommuteNumberLine
Login Mode → Check TC Device To Login Agent	ConfigurationDialog_SettingsTab_LoginMode_CheckTCDevice	ConfigurationDialog_PreferencesTab_CheckTCDeviceCheckBox
DTMF	ConfigurationDialog_SettingsTab_DTMF	ConfigurationDialog_PreferencesTab_typeOfDTMFGroupBox
DTMF → Comma Dialing Delay (msecs)	ConfigurationDialog_SettingsTab_DTMF_DTMFCommaDelay	
DTMF → DTMF Type	ConfigurationDialog_SettingsTab_DTMF_DTMFType	ConfigurationDialog_PreferencesTab_DTMFTypeComboBox
Conference	ConfigurationDialog_SettingsTab_Conference	
Conference → Use Consultative Type of Conference	ConfigurationDialog_SettingsTab_Conference_Consultative	ConfigurationDialog_PreferencesTab_ConferenceTypeComboBox
Transfer	ConfigurationDialog_SettingsTab_Transfer	
Transfer → Use Consultative Type of Transfer	ConfigurationDialog_SettingsTab_Transfer_Consultative	ConfigurationDialog_PreferencesTab_TransferTypeComboBox
Startup Message	ConfigurationDialog_SettingsTab_StartupMessage ConfigurationDialog_SettingsTab_StartupMessage_Message	ConfigurationDialog_PreferencesTab_StartupMessageGroupBox

Table continues…

UI control placement	UI control name	Control Names from 1.7 Release (It can also be used to lock this control)
Audio Output	ConfigurationDialog_SettingsTab_AudioOutput ConfigurationDialog_SettingsTab_AudioOutput_AudioOutput	ConfigurationDialog_AudioTab_audioOutputGroupBox ConfigurationDialog_AudioTab_AudioOutputDeviceComboBox ConfigurationDialog_AudioTab_AudioOutputVolumeSlider ConfigurationDialog_AudioTab_AudioOutputTestButton ConfigurationDialog_AudioTab_AudioOutputVolumeIndicator
Ringer Output	ConfigurationDialog_SettingsTab_RingerOutput ConfigurationDialog_SettingsTab_RingerOutput_RingerOutput	ConfigurationDialog_AudioTab_ringerOutputGroupBox ConfigurationDialog_AudioTab_RingerOutputDeviceComboBox ConfigurationDialog_AudioTab_RingerOutputVolumeSlider ConfigurationDialog_AudioTab_RingerOutputTestButton ConfigurationDialog_AudioTab_RingerOutputVolumeIndicator
Audio Input	ConfigurationDialog_SettingsTab_AudioInput ConfigurationDialog_SettingsTab_AudioInput_AudioInput	ConfigurationDialog_AudioTab_audioInputGroupBox ConfigurationDialog_AudioTab_AudioInputDeviceComboBox ConfigurationDialog_AudioTab_AudioInputVolumeSlider ConfigurationDialog_AudioTab_AudioInputTestButton ConfigurationDialog_AudioTab_AudioInputVolumeIndicator
Advanced Audio Settings	ConfigurationDialog_SettingsTab_AudioAdvanced	
Advanced Audio Settings → Headset Integration	ConfigurationDialog_SettingsTab_AudioAdvanced_HeadsetIntegration	ConfigurationDialog_AudioTab_headsetIntegrationCheckBox
Advanced Audio Settings → Control Device	ConfigurationDialog_SettingsTab_AudioAdvanced_ControlDevice	ConfigurationDialog_AudioTab_ControlDeviceComboBox

Table continues…

UI control placement	UI control name	Control Names from 1.7 Release (It can also be used to lock this control)
Advanced Audio Settings → Call Button	ConfigurationDialog_SettingsTab_AudioAdvanced_CallButton	ConfigurationDialog_AudioTab_ChooseCallButtonFuncComboBox
Advanced Audio Settings → Noise Suppression	ConfigurationDialog_SettingsTab_AudioAdvanced_NoiseSuppression	ConfigurationDialog_AudioTab_NoiseSupComboBox
Advanced Audio Settings → Auto Gain Control	ConfigurationDialog_SettingsTab_AudioAdvanced_AGC	ConfigurationDialog_AudioTab_AGCCheckBox
Advanced Audio Settings → Echo Cancellation	ConfigurationDialog_SettingsTab_AudioAdvanced_EchoCancellation	ConfigurationDialog_AudioTab_EchoCheckBox
Advanced Audio Settings → iTunes Control	ConfigurationDialog_SettingsTab_AudioAdvanced_EnableiTunesControl	ConfigurationDialog_AudioTab_ITunesControlCheckBox
EnableiTunesControl	ConfigurationDialog_AudioTab_ITunesControlCheckBox	
Message Waiting Indicator	ConfigurationDialog_SettingsTab_MWI	ConfigurationDialog_PreferencesTab_MWIGroupBox
Message Waiting Indicator → Show Message Waiting Indicator	ConfigurationDialog_SettingsTab_MWI_ShowMWI	ConfigurationDialog_PreferencesTab_EnableVoiceMessageLine
Message Waiting Indicator → Voice Mail Number	ConfigurationDialog_SettingsTab_MWI_VoiceNumber	ConfigurationDialog_PreferencesTab_VoiceNumberLine
Password Storage	ConfigurationDialog_SettingsTab_PasswordStorage	ConfigurationDialog_AdvancedTab_AllowNonSecurePasswordStorageCheckBox ConfigurationDialog_SecurityTab_PasswordStorageGroupBox
Password Storage → Password Storage Mode	ConfigurationDialog_SettingsTab_PasswordStorage_Mode	ConfigurationDialog_AdvancedTab_AllowNonSecurePasswordStorageCheckBox
PPM	ConfigurationDialog_SettingsTab_PPM	ConfigurationDialog_AdvancedTab_PPMGroupBox ConfigurationDialog_SecurityTab_PPMGroupBox
PPM → PPM Secure Mode	ConfigurationDialog_SettingsTab_PPM_PPMSecureMode	
Certificates Remote Host	ConfigurationDialog_SettingsTab_CertRemoteHost	

Table continues…

UI control placement	UI control name	Control Names from 1.7 Release (It can also be used to lock this control)
Certificates Remote Host → Remote Protocol	ConfigurationDialog_SettingsTab_CertRemoteHost_RemoteProtocol	
Certificates Remote Host → Remote Address	ConfigurationDialog_SettingsTab_CertRemoteHost_RemoteAddress	
Certificates Remote Host → Remote Port	ConfigurationDialog_SettingsTab_CertRemoteHost_RemotePort	
Third-Party Certification	ConfigurationDialog_SettingsTab_ThirdPartyCert	ConfigurationDialog_AdvancedTab_ThirdPartyCertsGroupBox ConfigurationDialog_SecurityTab_ThirdPartyCertsGroupBox
Third-Party Certification → Certification Mode	ConfigurationDialog_SettingsTab_ThirdPartyCert_CertMode	
Third-Party Certification → Certificates	ConfigurationDialog_SettingsTab_ThirdPartyCert_CertList	
Identity Certification	ConfigurationDialog_SettingsTab_IdentityCert	
Identity Certification → Certification Mode	ConfigurationDialog_SettingsTab_IdentityCert_IdentityCertMode	
Identity Certification → Certificate Path	ConfigurationDialog_SettingsTab_IdentityCert_IdentityCertPath	
Identity Certification → Certificate Password	ConfigurationDialog_SettingsTab_IdentityCert_IdentityCertPassword	
Identity Certification → Save Certificate Password	ConfigurationDialog_SettingsTab_IdentityCert_SavePassword	
Identity Certification → Certificate Authority URL	ConfigurationDialog_SettingsTab_IdentityCert_CertificateAuthorityUrl	
Identity Certification → Certificate Authority Password	ConfigurationDialog_SettingsTab_IdentityCert_CertificateAuthorityPassword	
Identity Certification → Common Name	ConfigurationDialog_SettingsTab_IdentityCert_IdentityCommonName	
Identity Certification → Distinguished Name	ConfigurationDialog_SettingsTab_IdentityCert_IdentityDistName	
Identity Certification → Key Length	ConfigurationDialog_SettingsTab_IdentityCert_IdentityKeyLength	

Table continues…

UI control placement	UI control name	Control Names from 1.7 Release (It can also be used to lock this control)
SRTP	ConfigurationDialog_SettingsTab_SRTP	ConfigurationDialog_AdvancedTab_SRTPGroupBox ConfigurationDialog_SecurityTab_SRTPGroupBox
SRTP → Enable SRTP	ConfigurationDialog_SettingsTab_SRTP_EnableSRTP	
SRTP → Media Encryption Parameters	ConfigurationDialog_SettingsTab_SRTP_EncryptionParameters	
Encryption Parameters		
SRTP → Enable SRTCP	ConfigurationDialog_SettingsTab_SRTP_SRTCP	
Internal Browser	ConfigurationDialog_SettingsTab_InternalBrowser	
Internal Browser → Ignore All SSL Errors in Browser	ConfigurationDialog_SettingsTab_InternalBrowser_IgnoreSSLErrors	
Internal Browser → Use Internal Browser for ACM Screen Pops by Default	ConfigurationDialog_SettingsTab_InternalBrowser_UseInternalBrowser	
ACM	ConfigurationDialog_SettingsTab_ACM	ConfigurationDialog_SecurityTab_ACMGroupBox
ACM → Ignore All SSL Errors from Internal Browser	ConfigurationDialog_SettingsTab_ACM_IgnoreACMErrors	
Session Manager	ConfigurationDialog_SettingsTab_SessionManager	
Session Manager → Failed Session Removal Timeout	ConfigurationDialog_SettingsTab_SessionManager_FailedSessionRemovalTimeout	
Session Manager → Enable Local Media Shuffling	ConfigurationDialog_SettingsTab_SessionManager_LocalMediaShuffling	
Language	ConfigurationDialog_SettingsTab_Language	ConfigurationDialog_AdvancedTab_languageGroupBox
Language → Language	ConfigurationDialog_SettingsTab_Language_Language	ConfigurationDialog_AdvancedTab_LocaleComboBox
Logging	ConfigurationDialog_SettingsTab_Logging	ConfigurationDialog_AdvancedTab_loggingGroupBox
Logging → Log Directory	ConfigurationDialog_SettingsTab_Logging_LogDir	

Table continues…

UI control placement	UI control name	Control Names from 1.7 Release (It can also be used to lock this control)
Logging → Log Level	ConfigurationDialog_SettingsTab_Logging_LogLevel	ConfigurationDialog_AdvancedTab_LogLevelComboBox
Logging → Maximum Log Files Size (in MB)	ConfigurationDialog_SettingsTab_Logging_MaxLogSize	
Logging → Include Media Logs	ConfigurationDialog_SettingsTab_Logging_IncludeMedia	ConfigurationDialog_AdvancedTab_EnableMediaQualityLoggingCheckBox
Logging → Enable Remote Logging	ConfigurationDialog_SettingsTab_Logging_EnableRemoteLogging	ConfigurationDialog_AdvancedTab_EnableRemoteLoggingCheckBox
Logging → Remote Logging Server	ConfigurationDialog_SettingsTab_Logging_RemoteLogServer	ConfigurationDialog_AdvancedTab_RemoteLoggingServerLineEdit
Logging → Remote Log Level	ConfigurationDialog_SettingsTab_Logging_RemoteLogLevel	ConfigurationDialog_AdvancedTab_RemoteLogLevelComboBox
Quality of Service Tagging	ConfigurationDialog_SettingsTab_QoS	ConfigurationDialog_AdvancedTab_QoSGroupBox
Quality of Service Tagging → Use Local QoS Settings	ConfigurationDialog_SettingsTab_QoS_UseLocalQoS	ConfigurationDialog_AdvancedTab_LocalQoSSettingsCheckBox
Quality of Service Tagging → Tag DSCP for Audio	ConfigurationDialog_SettingsTab_QoS_EnableAudioDSCP	ConfigurationDialog_AdvancedTab_DSCPCheckBox
Quality of Service Tagging → Tag DSCP for Signaling	ConfigurationDialog_SettingsTab_QoS_EnableSigDSCP	ConfigurationDialog_AdvancedTab_DSCPSigCheckBox
Quality of Service Tagging → Tag 802.1p for Audio	ConfigurationDialog_SettingsTab_QoS_EnableAudio802	ConfigurationDialog_AdvancedTab_Priority802_1CheckBox
Quality of Service Tagging → Tag 802.1p for Signaling	ConfigurationDialog_SettingsTab_QoS_EnableSig802	ConfigurationDialog_AdvancedTab_Priority802_1SigCheckBox
Quality of Service Tagging → DSCP Value for Audio	ConfigurationDialog_SettingsTab_QoS_AudioDSCP	ConfigurationDialog_AdvancedTab_DSCPLineEdit
Quality of Service Tagging → DSCP Value for Signaling	ConfigurationDialog_SettingsTab_QoS_SigDSCP	ConfigurationDialog_AdvancedTab_DSCPSigLineEdit
Quality of Service Tagging -> 802.1p Value for Audio	ConfigurationDialog_SettingsTab_QoS_Audio802	ConfigurationDialog_AdvancedTab_Priority802_1LineEdit
Quality of Service Tagging -> 802.1p Value for Signaling	ConfigurationDialog_SettingsTab_QoS_Sig802	ConfigurationDialog_AdvancedTab_Priority802_1SigLineEdit
Presence	ConfigurationDialog_SettingsTab_Presence	
Presence → Enable Presence	ConfigurationDialog_SettingsTab_Presence_EnablePresence	

Table continues…

UI control placement	UI control name	Control Names from 1.7 Release (It can also be used to lock this control)
RTCP Monitoring	ConfigurationDialog_SettingsTab_RTCP	
RTCP Monitoring → Server Address	ConfigurationDialog_SettingsTab_RTCP_Server	
RTCP Monitoring → Server Port	ConfigurationDialog_SettingsTab_RTCP_Port	
RTCP Monitoring → Monitoring Period	ConfigurationDialog_SettingsTab_RTCP_Period	
Extended Validation	ConfigurationDialog_SettingsTab_ExtendedValidation	
Extended Validation → Hostname Validation	ConfigurationDialog_SettingsTab_ExtendedValidation_HostnameValidation	
Extended Validation → Domain Validation	ConfigurationDialog_SettingsTab_ExtendedValidation_DomainValidation	
Legal	ConfigurationDialog_SettingsTab_Legal	
Legal → EULA	ConfigurationDialog_SettingsTab_Legal_EULA	
Key Strokes	ConfigurationDialog_SettingsTab_KeyStrokes	

Table continues…

UI control placement	UI control name	Control Names from 1.7 Release (It can also be used to lock this control)
Key Strokes items	ConfigurationDialog_SettingsTab_KeyStrokes_ACMLogout ConfigurationDialog_SettingsTab_KeyStrokes_ActivateSearch ConfigurationDialog_SettingsTab_KeyStrokes_ACWMode ConfigurationDialog_SettingsTab_KeyStrokes_AddContact ConfigurationDialog_SettingsTab_KeyStrokes_AddContactToConference ConfigurationDialog_SettingsTab_KeyStrokes_AgentLogout ConfigurationDialog_SettingsTab_KeyStrokes_AnswerCall ConfigurationDialog_SettingsTab_KeyStrokes_AnswerCallDuringActive ConfigurationDialog_SettingsTab_KeyStrokes_AuxMode ConfigurationDialog_SettingsTab_KeyStrokes_Conference ConfigurationDialog_SettingsTab_KeyStrokes_DeleteContact ConfigurationDialog_SettingsTab_KeyStrokes_DNDMode ConfigurationDialog_SettingsTab_KeyStrokes_EditContact ConfigurationDialog_SettingsTab_KeyStrokes_EndCall ConfigurationDialog_SettingsTab_KeyStrokes_HoldCall ConfigurationDialog_SettingsTab_KeyStrokes_ListenMailbox ConfigurationDialog_SettingsTab_KeyStrokes_MakeCall	

UI control placement	UI control name	Control Names from 1.7 Release (It can also be used to lock this control)
	ConfigurationDialog_SettingsTab_KeyStrokes_MakeCallToContact ConfigurationDialog_SettingsTab_KeyStrokes_Mute ConfigurationDialog_SettingsTab_KeyStrokes_OpenBrowser ConfigurationDialog_SettingsTab_KeyStrokes_OpenConfiguration ConfigurationDialog_SettingsTab_KeyStrokes_OpenContacts ConfigurationDialog_SettingsTab_KeyStrokes_OpenDialPad ConfigurationDialog_SettingsTab_KeyStrokes_OpenFeatureButtons ConfigurationDialog_SettingsTab_KeyStrokes_OpenHistory ConfigurationDialog_SettingsTab_KeyStrokes_OpenLoginDialog ConfigurationDialog_SettingsTab_KeyStrokes_OpenMediaQuality ConfigurationDialog_SettingsTab_KeyStrokes_OpenStatsConsole ConfigurationDialog_SettingsTab_KeyStrokes_Quit ConfigurationDialog_SettingsTab_KeyStrokes_ReadyMode ConfigurationDialog_SettingsTab_KeyStrokes_RegisterAgent ConfigurationDialog_SettingsTab_KeyStrokes_SaveLogsAs ConfigurationDialog_SettingsTab_KeyStrokes_StartSOWithContact ConfigurationDialog_SettingsTab_KeyStrokes_StationLogout ConfigurationDialog_SettingsTab_KeyStrokes_SwapCalls	

UI control placement	UI control name	Control Names from 1.7 Release (It can also be used to lock this control)
	ConfigurationDialog_SettingsTab_KeyStrokes_TerminateActiveAndAnswer ConfigurationDialog_SettingsTab_KeyStrokes_TerminateAllCalls ConfigurationDialog_SettingsTab_KeyStrokes_TerminateCallAndUnhold ConfigurationDialog_SettingsTab_KeyStrokes_TransferCall ConfigurationDialog_SettingsTab_KeyStrokes_TransferCallToContact ConfigurationDialog_SettingsTab_KeyStrokes_VolumeDown ConfigurationDialog_SettingsTab_KeyStrokes_VolumeOnOff ConfigurationDialog_SettingsTab_KeyStrokes_VolumeUp	

Reason Codes Tab

UI control placement	UI control name
Reason Codes Tab → Reason Code Types	ConfigurationDialog_ReasonCodesTab
Reason Codes Tab → Add new code button	ConfigurationDialog_ReasonCodesTab_AddItemBtn
Reason Codes Tab → Remove Button	ConfigurationDialog_ReasonCodesTab_RemoveBtn
Reason Codes Tab → Reason Codes table control	ConfigurationDialog_ReasonCodesTab_TableView
Reason Codes Tab → Reason Codes column header	ConfigurationDialog_ReasonCodesTab_TableViewHeader

Greetings Tab

UI control placement	UI control name
Greetings Tab	ConfigurationDialog_GreetingsTab
Greetings Tab → Control group name (header)	ConfigurationDialog_SettingsTab_GreetingsSettings_Header
Greetings Tab → Add button	ConfigurationDialog_GreetingsTab_AddBtn
Greetings Tab → Remove button	ConfigurationDialog_GreetingsTab_RemoveBtn

Table continues…

UI control placement	UI control name
Greetings Tab → Up button	ConfigurationDialog_GreetingsTab_UpBtn
Greetings Tab → Down button	ConfigurationDialog_GreetingsTab_DownBtn
Greetings Tab → Sidebar (greetings list)	ConfigurationDialog_GreetingsTab_TableView ConfigurationDialog_GreetingsTab_TableViewHeader
Greetings Tab → All Controls for Greeting Editing	ConfigurationDialog_SettingsTab_GreetingsSettings
Greetings Tab → Rule Name	ConfigurationDialog_SettingsTab_GreetingsSettings_RuleName
Greetings Tab → VDN Name Pattern	ConfigurationDialog_SettingsTab_GreetingsSettings_VDNPattren
Greetings Tab → Auto Play only if	ConfigurationDialog_SettingsTab_GreetingsSettings_AutoPlay
Greetings Tab → File Path	ConfigurationDialog_SettingsTab_GreetingsSettings_FilePath
Greetings Tab → File Name	ConfigurationDialog_SettingsTab_GreetingsSettings_FileName
Greetings Tab → Recording	ConfigurationDialog_SettingsTab_GreetingsSettings_Recording
Greetings Tab → Duration	ConfigurationDialog_SettingsTab_GreetingsSettings_Duration

Screen Pop Tab

UI control placement	UI control name
Screen Pop Tab	ConfigurationDialog_ScreenPopTab
Screen Pop Tab → Add button	m_pScreenPopAddBtn
Screen Pop Tab → Remove button	m_pScreenPopRemoveBtn
Greetings Tab → All Controlls for Screen Pop Editing	ConfigurationDialog_SettingsTab_ScreenPopSettings
Screen Pop Tab → Rule Name	ConfigurationDialog_SettingsTab_ScreenPopSettings_RuleName
Screen Pop Tab → Type	ConfigurationDialog_SettingsTab_ScreenPopSettings_Type
Screen Pop Tab → URL	ConfigurationDialog_SettingsTab_ScreenPopSettings_Url
Screen Pop Tab → Parameters	ConfigurationDialog_SettingsTab_ScreenPopSettings_Parameters
Screen Pop Tab → Trigger	ConfigurationDialog_SettingsTab_ScreenPopSettings_Trigger

Table continues…

UI control placement	UI control name
Screen Pop Tab → Trigger Only for ACD calls	ConfigurationDialog_SettingsTab_ScreenPopSettings_TriggerIfVDN
Screen Pop Tab → VDN Name	ConfigurationDialog_SettingsTab_ScreenPopSettings_VDN
Screen Pop Tab → Application	ConfigurationDialog_SettingsTab_ScreenPopSettings_Application
Screen Pop Tab → control group name (header)	ConfigurationDialog_SettingsTab_ScreenPopSettings_Header

Invoking Avaya Agent for Desktop in Citrix or VMWare Horizon environments

Before you begin

Ensure that you have already installed Avaya Agent for Desktop on the Citrix or VMWare Horizon server.

Note:

For Citrix and VMWare Horizon, you must use Avaya Agent for Desktop in a Desk phone mode.

Procedure

1. Log in into Citrix or VMWare Horizon receiver.
2. Navigate and double-click the Avaya Agent for Desktop icon on the required tab, such as Desktops or APPS as applicable.
3. Follow the Avaya Agent for Desktop login procedure.

   For more details on login procedures, see *Using Avaya Agent for Desktop guide* on the Avaya support portal

Key Strokes field descriptions

Configure the **Key Strokes** commands for each of the following functions. These keystroke commands must be combination of the alphabets or the numbers with the special keys Alt, Ctrl, or Shift only. For example, Shift+Ctrl+A or Ctrl+1. You must keep these keys pressed to add combination values in the given **Key Strokes** fields.

Note:

You can choose to use the default keystroke commands or define your own commands for the given list of functions.

Name	Description
Key Strokes	The fields to view or define the keystroke commands for the given list of Avaya Agent for Desktop functions. These settings when combined with the compatible assistive technology, such as JAWS, makes the application accessible for the blind users. The available options are: • **ACM/AADS Logout** • **After Call Work Mode** • **Activate Search** • **Add Contact** • **Add Contact to Conference** • **Answer Ringing Call During Active Call** • **Answer Call** • **Answer Ringing Call During Active Call** • **Aux Mode** • **Create Conference** • **Do not disturb** • **Delete contact** • **Edit contact** • **End Call** • **Hold Call** • **Listen Mailbox** • **Make Call** • **Make Call to Contact** • **Mute/UnMute** • **Open Browser** • **Open Configuration** • **Open Contacts** • **Open Dial Pad** • **Open Feature Buttons** • **Open History** • **Open Login Dialog** • **Open Media Quality** • **Open Stats Console**

Name	Description
	• **Quit** • **Ready Mode** • **Register Agent** • **Save Logs As** • **Start Service Observing with Contact** • **Station Logout** • **Switch between Held Call and Active Call** • **End Active Call And Answer Incomming Call** • **End All Calls** • **End Active Call and Unhold Other Call**

Related links

Configuring the Key Strokes settings on page 164

Configuring the Key Strokes settings

About this task

Using the **Key Strokes** commands, you can use the shortcut keys to perform given functions in the **Key Strokes** settings. These keystroke commands must be combination of the alphabets or the numbers with the special keys Alt, Ctrl, or Shift only. For example, Shift+Ctrl+A or Ctrl+1. You must keep these keys pressed to add combination values in the given **Key Strokes** fields.

Note:

You can choose to use the default keystroke commands or define your own commands for the given list of functions.

Procedure

1. In the system try, right-click the Avaya Agent for Desktop icon and select **Settings**.

   The system displays the Avaya Agent for Desktop Settings window.
2. On the **Settings** tab, click the **Key Strokes** menu.
3. In the **Key Strokes** section, add values for the required functions in the given list.
4. Click **Save**.
5. Restart the Avaya Agent for Desktop application.

Related links

Key Strokes field descriptions on page 162

Avaya Aura® Device Services (AADS) support overview

Feature overview

Avaya Agent for Desktop supports various services of Avaya Aura®Device Services (AADS). Avaya Agent for Desktop can retrieve configuration and login credentials using the external AADS configuration server. The AADS server available environment can be discovered using a DNS service resolution feature. Depending on the environment, there are following two ways to login to AADS server:

- **Basic authentication**: Here, Avaya Agent for Desktop requests users to provide the email address or AADS server direct URL of the third-party service. The AADS server sends back the configuration details if the login details are entered correctly. On next step, user needs to provide AADS login and password on Avaya Agent for Desktop main login window.
- **Third-party authentication using OAuth2 SAML**: Here, Avaya Agent for Desktop requests users to provide the email address or AADS server direct URL of the third-party service. Once inputs are provided, Avaya Agent for Desktop redirects agents to third-party login screen. On next step, user needs to provide login and password on the third-party OAuth2 SAML authorization login window. This is implemented using the OAuth2 protocol and Security Assertion Markup Language (SAML) authentication method. If login is successful, OAuth2 SAML authorization window is closed, and user is returned to the Avaya Agent for Desktop main login window. Here, the user is allowed to continue logging in Station and Agent, otherwise user is returned to the intial step of the AADS login.

  Note:

  - Avaya Agent for Desktop currently supports only SIP for AADS.
  - For sequence diagram and other details about AADS, see *Administering Avaya Aura® Device Services* documentation on the Avaya support site.

Avaya Agent for Desktop Preferred SAML login type user experience:

- **Preferred SAML login type is active**: When **AAFD Preferred SAML login type** feature is enabled, AADS login is changed to "`bearer`" forcibly even if service supports "basic" sign in. So, user can enter URL without specific `?preferredAuth=bearer` add-on to the initial request URL. If `bearer` sign in fails, user can perform `basic` sign in. The same algorithm is applied to e-mail user input type sign in.
- **Preferred SAML login type is inactive**: When **AAFD Preferred SAML login type** feature is enabled, but `?preferredAuth=bearer` is not there in the user input URL, then sign in fails. If service supports "basic" sign in, but `?preferredAuth=bearer` is there in user input URL, then sign in fails.

Avaya Agent for Desktop Preferred SAML use cases:

- AADS login is successful when Preferred SAML flag is set to active with URL with `?preferredAuth=bearer`.
- AADS login is successful when Preferred SAML flag is set to active with URL without `?preferredAuth=bearer` in address, but server supports `bearer` sign in.
- AADS login is successful when Preferred SAML flag is set to active with e-mail.
- AADS login is successful when Preferred SAML flag is set to active with non-SAML(basic) URL.

- AADS login is successful when Preferred SAML flag is set to active with SAML URL, but server does not support SAML.

Revoking access using O-Auth/SAML

Administrators or supervisors have ability to revoke access for a particular agent by controlling Third-party SAML identity provider. If access is revoked for an agent, the agent is notified and signed out from the Avaya Agent for Desktop application.

Avaya Agent for Desktop keeps AADS O-Auth or SAML session active to monitor user access. If any connectivity issue occurs, then Avaya Agent for Desktop cannot control the access anymore. In such cases, Avaya Agent for Desktop notifies the user that the current session will be over soon due to AADS disconnection issue. Avaya Agent for Desktop provides one hour grace period to restore the connection. If the connection cannot be restored, then Avaya Agent for Desktop signs out the agent.

Note:

To create Avaya Agent for Desktop client mapping in AADS, see *Creating client mapping* section in the *Administering Avaya Aura® Device Services* guide on the Avaya support site.

Adding Avaya Agent for Desktop specific settings on AADS

Procedure

1. Log in to Avaya Aura® System Manager and create a user instance.
2. Create a **Communication Profile** on the **Other Email** tab, where the profile name for the AADS server must be specified.
3. On the **Identity** tab, the **User Provisioning Rule** must be set to **Auto**.
4. Log in to the AADS admin portal and add/update parameters.
5. The resulting configuration file content must be checked by opening the AADS configuration URL in the browser. Here, users must log in with the user credentials created on Avaya Aura® System Manager, or otherwise enter the user name provided in the **Other Email** field.

   Note:

   For more details, see *Administering Avaya Aura® System Manager* and *Administering Avaya Aura® Device Services* on the Avaya support site.

List of supported Avaya Agent for Desktop settings on AADS

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
Ignore All SSL Errors with AADS	IGNORE_SSL_ERR_AADS	Default: 0 Possible values: 0,1	-	Internal parameter only.
License Server URL	LICENSE_SERVER_URL	Default: https://WebLMhost:52233/WebLM/LicenseServer Possible values: https URL address	-	License server URL. This parameter is applied and is visible in Configuration manager, but remains default in startconfig.ini.
Signaling	SIP_SIGNALING	Default: SIP Possible values: SIP, H323	-	This parameter requires reboot.
• Primary SIP Proxy Address • Primary Server Port • Primary Transport • Secondary SIP Proxy Address • Secondary Server Port Secondary Transport	SIP_CONTROLLER_LIST	Default: None Possible values for: • SIP Proxy addresses: String in appropriate format • Server ports: 0 - 65535 • Transport protocols: TLS, TCP, UDP	SIP_CONTROLLER_LIST format: host[:port][;transport=xxx] Example: SET SIP_CONTROLLER_LIST "proxy1:5061;transport=tls,proxy2:5061;transport=tls"	The SIP_CONTROLLER_LIST in the settings file specifies a list of SIP controller designators, separated by commas without any intervening spaces
SIP domain	SIPDOMAIN	Default: None Possible values: Domain string	-	The SIP domain

Table continues…

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
Number of Connection Attempts to CM/SM	MAX_LOGIN_ATTEMPTS	Default: 3 Possible values: 1 to 5	-	Max number of connection attempts to CM/SM. Maximum 3 attempts are recommended, but you can keep this number as per your requirement.
Communication Manager Auto Answer Support Required	CM_AUTO_ANSWER_SUPPORT_REQUIRED	Default: 1 Possible values: 0,1	-	Communication Manager Auto Answer Support Required
Communication Manager Onhook Dialing Support Required	CM_ONHOOK_DIALING_SUPPORT_REQUIRED	Set to 0 or 1	-	In H.323 mode, this parameter is used for Communication Manager Onhook Dialing. This setting must be enabled when "Onhook dialing on Terminal" is set to Y on the Communication Manager. If set to Y, the # key is not added for 1 digit reason codes. Otherwise, the key is added.
Communication Manager Forced type of Aux Reason Code Support Required	CM_FORCED_AUX_SUPPORT_REQUIRED	Set to 0 or 1		This setting must be enabled when Aux Work Reason Code Type is set to "Forced" on Communication Manager. In this case manual usage of Default (0) Aux code is restricted by Avaya Agent for Desktop.
Directory Address	DIRSRVR	Default: None Possible values: IP address or domain name	-	The IP address or fully qualified domain name of the LDAP server.

Table continues…

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
Directory Port	DIRSRVRPRT	Default: 389 Possible values: 0 - 65535	-	Port number for LDAP server
Directory Root Search	DIRTOPDN	Default: None Possible values: N/A	-	LDAP search base
Directory Username	DIRUSERNAME	Default: None Possible values: Authentication username	-	LDAP authentication username
Directory Password	DIRPASSWORD	Default: None Possible values: Authentication password	-	LDAP authentication password
Save Directory Password	DIRPASSWORD_SAVE	Default: 1 Possible values: 0,1	-	Save Directory Password
Bind Option	DIRBIND_OPTION	Default: Simple Possible values: Simple, GSS Bind	-	-
Enable Dialing Rules	ENHDIALSTAT	Default: 1 Possible values: 0, 1	-	The parameter that indicates whether dialing rules are enabled. The options are: 1: Indicates enabled. 0: Indicates disabled.
Internal Extension Length	PHNDPLENGTH	Default: 5 Possibe values: 3 - 16	-	The internal extension length
Local Calling Area Codes	DIALPLANAREACODE	Default: None Possible values: As per the required area code	-	The area or city code

Table continues…

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
Length of National Phone Numbers	PHNLDLENGTH	Default: 10 Possible values: As per your country's national phone number length	-	The length of national phone numbers
Number To Dial To Access External Numbers	PHNOL	Default: 9 Possible values: As per the requirement	-	The number to dial to access an external line
Number To Dial To International Calls	PHNIC	Default: 11 Possible values: As per the requirement	-	The number to dial for international calls
Number to Dial for Long Distance Calls	PHNLD	Default: 1 Possible values: As per the requirement	-	The number to dial for long distance calls
Your Country Code	PHNCC	Default: 1 Possible values: 0-999	-	The country code
Use Only User Regular Expression	CLICK_TO_DIAL_FORCE_USER_REGEXP	Default: 0 Possible values: 0, 1	-	User Regular Expression
Regular Expression	CLICK_TO_DIAL_REGEXP	Default: None Possible values: Regular expression string	-	-
Exclusion List	CLICK_TO_DIAL_EXCL_LIST	Possible values: "URL1 URL2 URL3"	-	-
Ready Mode	AGENT_AVAILABILITY_AUTO	Default: 0 Possible values: 0, 1	-	Used to check if an agent is in a manual/auto work mode. '1' is Auto-in, '0' is manual-in.
Timed After Call Work	AGENT_TIMED_ACW	Default: 0 Possible values: 0, 1	-	Timed After Call Work
After Call work Duration (seconds)	AGENT_TIMED_ACW_DURATION	Default: 0 Possible values: 0-65535	-	After Call work Duration (seconds)

Table continues…

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
Allow Manual After Call Work	AGENT_DISABLE_ACW	Default: 0 Possible values: 0, 1	-	Used to disable agents
Agent state upon the login	AGENT_STATE_UPON_LOGIN	Default: 1 Possible values: 0, 1	-	0 - Ready, 1 - Aux
Agent state auto recovery timer	AGENT_STATE_AUTO_RECOVERY_TIMER	Default: 60 Possible values: 0-86400	-	In seconds. For network issues shorter than timer, the agent state will be restored despite server commands, after timer expiry the state will depend on the server set state.
Automatically Login the Agent	AUTO_LOGIN_AGENT	Default: 0 Possible values: 0, 1	-	EC parameter name: AUTO_LOGIN_FLAG
Automatically Login the Station	AUTO_LOGIN_STATION	Default: 0 Possible values: 0, 1	-	-
Launch Avaya Agent when Windows Starts	APPLICATION_AUTO_START	Default: 0 Possible values: 0, 1	-	Auto Start. Options for this setting are: 0 = NO, 1 = YES
Show User Interface	SHOW_UI	Default: 1 Possible values: 0, 1	-	== "Hide interface" check box in tray menu
Always Display the Main Window On Top	ALWAYS_ON_TOP	Default: 0 Possible values: 0, 1	-	Always Display the Main Window On Top
Local Auto Answer	LOCAL_AUTO_ANSWER	Default: 0 Possible values: 0, 1	-	Local Auto Answer
Stay In Notification Area If Main Window Is Closed	STAY_NOTIF_IF_MW_CLSD	Default: 1	-	-

Table continues…

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
Show WebLM Server Warning Messages	SHOW_WEBLM_SRV_WRN_MSG	Default: 1	-	-
Show Drop Call Button	SHOW_DROP_BTN	Default: 0 Possible values: 0, 1	-	-
Permanent Network error messages	PERMANENT_NETWORK_ERR_MSG	Default: 0 Possible values: 0, 1	-	-
Use random signaling port	USE_RANDOM_SIG_PORT	Default: 0 Possible values: 0, 1	-	-
Enable Network reconnect notification	ENABLE_NETWORK_RECONNECT_MSG	Default: 1 Possible values: 0, 1	-	-
Login Mode	LOGINMODE	Default: My Computer Possible values: My Computer, Deskphone, Other Phone	Example: SET LOGINMODE "My Computer"	login mode (AAfD mode)
Telecommuter Number	TC_NUMBER	Default: NA Possible values: Telecommuter contact number	-	Telecommuter Number
Check TC Device To Login Agent	TC_CHECK_TO_LOGIN_AGENT	Default: 0 Possible values: 0, 1	-	Check TC Device To Login Agent
Show Message Waiting Indicator	MWI_SHOW	Default: 0 Possible values: 0, 1	-	Show Message Waiting Indicator
Voice Mailbox Number	MWI_NUMBER	Default: NA Possible values: Voice mailbox contact number	-	Voice Mailbox Number

Table continues…

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
DTMF Type	DTMF_TYPE	Default: out-of-band Possible values: out-of-band, in-band, rtp-payload	-	-
Comma Dialing Delay (msecs)	DTMF_COMMA_DIALING_DELAY	Default: 1000 Possible values: 0-9999	-	Comma Dialing Delay (msecs)
Use Consultative Type of Conference	CONSULT_CONFERENCE	Default: 0 Possible values: 0, 1	-	Used for consultative type of conference
Use Consultative Type of Transfer	CONSULT_TRANSFER	Default: 0 Possible values: 0, 1	-	Used for consultative type of transfer
Use No Hold Type of Transfer	USE_NO_HOLD_TRANSFER_TYPE	Default: 1 Possible values: 0, 1	-	Do not enable for non-Aura environment
Use Consultative Type of Conference	USE_NO_HOLD_CONFERENCE_TYPE	Default: 1 Possible values: 0, 1	-	Used for non-consultative conference type
Startup Message	STARTUP_MSG	Default: None Possible values: Start up text message	-	Startup Message
Output Device	AUDIO_OUTPUT_NAME	Default: Remote Audio Possible values: NA	-	-
Output Volume	AUDIO_OUTPUT_VOL	Default: 50 Possible values: 0-100	-	Output Volume
Ringer Device	AUDIO_RINGER_NAME	Default: Remote Audio Possible values: NA	-	-
Ringer Volume	AUDIO_RINGER_VOL	Default: 50 Possible values: 0-100	-	Output Volume

Table continues…

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
Input Device	AUDIO_INPUT_NAME	Default: NA Possible values: NA	-	-
Input Volume	AUDIO_INPUT_VOL	Default: 50 Possible values: 0-100	-	Input Volume
Headset Integration	HEADSET_INTEGRATION	Default: Basic (HID API) Possible values: Disabled, Basic, Advanced	SET HEADSET_INTEGRATION Disabled|Basic|Advanced	The following parameters are used: Disabled Basic - for Basic (HID API) Advanced - for Advanced (SDK Native). Advanced is not supported for 64-bit version, Basic (HID API) will be selected
Control Device	CONTROL_DEVICE_NAME	Default: NA Possible values: Select available headset options	-	-
Call Button	HEADSET_CALL_BTN_ACTION	Default: Disabled Possible values: Disabled, Answer, Hold, Drop	-	-
Noise Suppression	NOISE_SUPPRESSION	Default: Disabled Possible values: Disabled, Conference, Low, Moderate, High, Very High	-	-
Auto Gain Control	ENABLE_AUTO_GAIN_CTRL	Default: 1 Possible values: 0, 1	-	Auto Gain Control

Table continues…

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
Echo Cancellation	ECHO_CANCELLATION	Default: 0 Possible values: 0, 1	-	The echo cancellation algorithm. Echo cancellation is a process that removes echo from a voice communication to improve voice quality on a telephone call. The supported values are: • aec: This is a default value. • aecm • off
Password Storage Mode	PASSW_STORAGE_MODE	Default: Security Storage Only Possible values: Security Storage Only, Security Storage if Available, Non-secure storage only	-	The user defined passwords are cached and may be restored back after AADS logout. Applicable only in case of Non-Secure storage mode. This parameter requires reboot.
PPM Secure Mode	PPM_SECURE_MODE	Default: HTTPS Possible values: HTTP, HTTPS	-	-
Certification Mode	THIRD_PARTY_CERT_MODE	Default: Not Used Possible values: Not Used, Use Local, Remote	-	This parameter requires reboot.

Table continues…

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
Certificates	TRUSTCERTS	Default: None Possible values: None	-	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 the various servers. Set a blank value to clear the private truststore and go back to the platform trust store. Certificates stored in binary DER form,commonly known as .cer, .crt, or .derfiles, and Base64-encoded DER form,commonly known as .pem files, are supported. This parameter requires reboot.
Remote Protocol, Remote Address, Remote Port	• CERT_REMOTE_PROTOCOL • CERT_REMOTE_ADDR • CERT_REMOTE_PORT	• Default: HTTPS, Possible values: HTTP, HTTPS • Default: None,Possible values: IP address URL • Default: None, Possible values: Port number for CERT server	-	These parameters require reboot. This is a part of the group of parameters that can only be set if they are all specified together to prevent inconsistent configuration of AAfD. The certificate mode (MYCERT_MODE) must be set to ‘Remote’ to allow this group of parameters to be set.

Table continues…

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
Certificate URL Download	MYCERT	Default: None Possible values: Certificate download URL	-	Example: http://example.com/cert/test.p12
Certification Mode	MYCERT_MODE	Default: None Possible values: Not Used, Use Local, Remote, Certificate Authority	-	This parameter requires reboot.
Certificate Path	MYCERT_PATH	Default: None Possible values: Certificate location path	-	-
Certificate Password	MYCERT_PASSWORD	Default: None Possible values: Certificate access password	-	-
Save Certificate Password	MYCERT_PASSWORD_SAVE	Default: 0 Possible values: 0,1	-	-
Certificate Authority URL	MYCERTURL	Default: None Possible values: Certificate authority URL	-	-
Certificate Authority Password	MYCERT_CA_PASSWORD	Default: None Possible values: Certificate authority password	-	-
Common Name	MYCERTCN	Default: None Possible values: Text for common certifcate name	-	-
Distinguished Name	MYCERTDN	Default: None Possible values: Text for common distinguished certificate name	-	-

Table continues…

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
Key Length	MYCERTKEYLEN	Default: None Possible values: 1024, 2048	-	-
Enable SRTP	ENABLE_SRTP	Default: 1 Possible values: 0, 1	-	This parameter requires reboot.
Enable SRTCP	ENABLE_SRTCP	Default: 0 Possible values: 0, 1	-	This parameter requires reboot.
Media Encryption Parameters	MEDIAENCRYPTION	Default: 9 Possible values: NA	-	This parameter enables the best effort SRTP with AES 128. You can also enable AES 256 by using the values from 0 to 9. This parameter requires a restart of the application.
Ignore All SSL Errors in Browser	IGNORE_SSL_ERR_BROWSER	Default: 0 Possible values: 0, 1	-	Ignore All SSL Errors in Browser
Language	SYSTEM_LANGUAGE	Default: 0 Possible values: 0, 1	-	This parameter requires reboot.
Log Directory	LOG_PATH	Default: NA Possible values: Directory path to save logs	-	Log Directory
Log Level	LOG_LEVEL	Default: Error Possible values: Error, Info, Debug	-	-
Maximum Log file size (in MB)	LOG_FILE_MAXSIZE	Default: 100 Possible values: NA	-	Maximum Log file size (in MB)
Include Media Quality Logs	ENABLE_MEDIA_LOG	Default: 1 Possible values: 0, 1	-	Include Media Quality Logs

Table continues…

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
Enable Remote Logging	REMOTE_LOG_ENABLED	Default: 0 Possible values: 0, 1	-	Enable Remote Logging
Remote Logging Server	REMOTE_LOG_SERVER	Default: NA Possible values: IP address URL	-	Remote Logging Server
Remote Log Level	REMOTE_LOG_LEVEL	Default: Error Possible values: Error, Info, Debug	-	-
Use Local QoS Settings	QOS_USE_LOCAL_CONFIG	Default: 0 Possible values: 0, 1	-	Quality of Service Local config
Tag DSCP for Audio	QOS_USE_AUDIO_DSCP	Default: 1 Possible values: 0, 1	-	Quality of Service Audio DSCP
DSCP Value for Audio	QOS_AUDIO_DSCP_VALUE	Default: 46 Possible values: 0-63	-	Quality of Service Audio DSCP Value
Tag DSCP for Signaling	QOS_USE_SIGNALING_DSCP	Default: 0 Possible values: 0, 1	-	Quality of Service Signaling DSCP
DSCP Value for Signaling	QOS_SIGNALING_DSCP_VALUE	Default: 46 Possible values: 0-63	-	Quality of Service Signaling DSCP Value
Tag 802.1p for Audio	QOS_USE_AUDIO_802_1	Default: 1 Possible values: 0, 1	-	Quality of Service AUDIO 802_1
802.1p Value for Audio	QOS_AUDIO_802_1_VALUE	Default: 6 Possible values: 0-7	-	Quality of Service AUDIO 802_1 Value
Tag 802.1p for Signaling	QOS_USE_SIGNALING_802_1	Default: 6 Possible values: 0-7	-	Quality of Service Signaling 802_1
802.1p Value for Signaling	QOS_SIGNALING_802_1_VALUE	Default: 6 Possible values: 0-7	-	Quality of Service Signaling 802_1 Value

Table continues…

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
Server Address	RTCPMON_SRV	Default: NA Possible values: IP address URL	-	RTCP Server Address
Server Port	RTCPMON_PORT	Default: 5005 Possible values: NA	-	RTCP Server Port
Monitoring Period	RTCPMON_PERIOD	Default: 5 Possible values: 0-30	-	RTCP Monitoring Period
Enable Presence	PRESENCE_ENABLED	Default: 0 Possible values: 0-2	-	Enable Presence

Table continues…

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
Auxiliary Reason codes	AUX_REASON_CODES DEFAULT_AUX_REASON_CODE	Default: None Possible values: None	Reason codes string format: "int:string,int:string, ..." Int code value should be a non-negative number. Additional restriction for AUX and Logout Reason codes: int code value should be less than 100. Invalid codes will be skipped. If 0 exists in int code values, then this reason code will be considered as default unless otherwise specified in "DEFAULT_*_CODE" parameter. If there is no 0 int code then the first reason code will be considered as default unless otherwise specified in "DEFAULT_*_CODE" parameter.	Example: SET AUX_REASON_CODES "1:default,02:break,3:outofofficeverylongauxcode,44:meeting,112:something 112,-22:semethingminus,888:big888,-5:minus5"
Log Out Reason Codes	LOGOUT_REASON_CODES DEFAULT_LOGOUT_REASON_CODE	Default: None Possible values: None	-	-
Call Work Codes	CALL_WORK_CODES DEFAULT_CALL_WORK_CODE	Default: None Possible values: None	-	-

Table continues…

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
List of Greetings Rules	GREETINGS_RULES	Default: None Possible values: None	Greetings string format: "param1=val1,param2=val2;param12=val12,param22=val22" Parameters of the one Greeting are divided by "," Greeting objects divided by ";" List of the parameters (* - required not-empty parameters): "description" - default: "New Greeting" [string] "autoplay" - default: "NOT-PLAY" [string from list: "NOT-PLAY", "AGENT-READY", "AGENT-LOGGEDIN", "INCOMING-CALL"] "filepath" - (*) [string] {Note: can be relative or absolute, in case of relative: Firstly, the search will start from AADS sounds directory and if the file is not here we will try to find it in default sounds dir} "vdn" - default: ""	Example: SET GREETINGS_RULES description=TestGreeting,autoplay=AGENT-LOGGEDIN,filepath=test.lbc
List of Greetings Files	GREETINGS_FILES	Default: None Possible values: None	-	-

Table continues…

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
List of Screen Pops	SCREEN_POP_LIST	Default: None Possible values: None	ScreenPop string format: "param1=val1,param2=val2;param12=val12,param22=val22" Parameters of the one ScreenPop are divided by "," 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] "type" - default: "EXTERNAL-BROWSER" [string from list: "APPLICATION", "INTERNAL-BROWSER", "EXTERNAL-BROWSER"] "trigger" - default: "INCOMING-RINGING" [string from list: "INCOMING-RINGING", "INCOMING-ANSWERED", "INCOMING-MISSED", "INCOMING-RELEASED", "OUTGOING-ESTABLISHED",	Exmaple: SET SCREEN_POP_LIST "name=ScreenPop1,type=APPLICATION,url=http://www.google.com,trigger=INCOMING-RINGING,triggerOnlyForVDN=0;"

Table continues…

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
			"OUTGOING-RELEASED"]	
LicenseType	0	Default: Advanced/ Standalone Possible values: 1-Basic, 2-Advaced/ Standalone, 3-Headless, 4-Deskphone	Example: SET LICENSE_TYPE 1	It can be selected by a user at the first launch only and cannot be changed after. But we need to allow to change it thru AADS. The new value, received from AADS is reflected in startcofig.ini. This parameter requires reboot.
Extension	SIPUSERNAME	Default: NA Possible values: Username string for SIP extension	-	The SIP account name
Extension Password	SIPPASSWORD	Default: NA Possible values: SIP extension username's password	-	The SIP account password
Agent	AGENT_LOGIN_ID	Default: NA Possible values: Agent Id string	-	Agent login id
Agent Password	AGENT_PASSWORD	Default: NA Possible values: Agent password string	-	Agent password
Hostname Validation	EXT_HOSTNAME_VALIDATION	Default: Disabled Possible values: 0, 1 or 2	"Disabled", "Informational" or "Enforced"	-
Domain Validation	EXT_DOMAIN_VALIDATION	Default: Disabled Possible values: 0, 1 or 2	"Disabled", "Informational" or "Enforced"	-
Failed Session Removal Timeout	FAILED_SESSION_REMOVAL_TIMEOUT	Default: 1 Possible values: 1 to 999	-	-

Table continues…

AAFD Setting Name	AADS Name	Default / Possible Values	Format	Comment
Enable Local Media Shuffling	SHUFFLING_ENABLED	Default: 0 Possible values: 0, 1	**Note:** Can be applied only for Telecommuter login mode	-
SIPHA1 for current user	SIPHA1	Default: NA Possible values: NA	-	Internal Avaya Agent for Desktop parameter. It does not show up in ConfigDialog.

Adding new attributes to the Global User level from import file

About this task

If you need to add multiple user keys at once, you need to import JSON file with all attributes.

Before you begin

Ensure that you have already downloaded the AADS defintion JSON file on your system. The AADS definition JSON file must be downloaded from Avaya's Product Licensing and Delivery System (PLDS) site -https://plds.avaya.com/

Procedure

1. Log in to AADS admin portal.
2. On the AADS panel, click **Dynamic Configuration** in the left menu.
3. Click **Configuration**.
4. In **Search Criteria**, ensure that **Configuration** option is selected.

   Note:

   You can select any one of the existing configurations or leave this option blank.
5. Click **Retrieve** to find Avaya Agent for Desktop AADS Settings of JSON file.
6. Provide **Name**, **Description**, **Type**, **Default value**, and **Version** to save the file on the local storage.
7. Click **Import**.
8. On the pop up window, **Select type of import** as **Import dynamic settings**.
9. Choose JSON file from your local storage and click **Import**.

   After successful import, you will see the keys added in all the tabs, such as **Global**, **Group**, **User**, and **Platform**.

10. Select your newly added key and publish your changes.
11. After all keys are selected, you must save the current configuration or create a new one.
12. On popup window, type your user credentials and click **Publish**.

Note:

If you want to make changes for a particular user only, the **User settings will be applied** check box must be selected. After clicking on **Publish**, your changes will be visible.

Enabling AADS login settings in Avaya Agent for Desktop

Procedure

1. In the Avaya Agent for Desktop Settings window, click the **Server** tab.
2. In the **AAFD Login Type** drop-down list, select **AADS Login**.
3. Chose from the following use cases for the **Preferred AADS SAML login type** check box:
   - If **Preferred AADS SAML login type** is selected: The application tries to use AADS SAML authentication before hand for all server types. In case of failure, application suggests basic authorization.
   - If **Preferred AADS SAML login type** is not selected: The application automatically selects the basic or SAML login type based on the user's AADS server URL format input.
4. Click **Save**.

DNS server configuration

DNS service resolution algorithm

The Avaya Agent for Desktop user needs to know the AADS server address to login to AADS and download settings. If the user do not know the AADS server URL, they can enter email address in the AADS login window instead of the direct AADS server URL.

Here, Avaya Agent for Desktop parses the entered domain and uses it in a query to the DNS server. The DNS Service Discovery (DNS-SD) protocol is used to retrieve the AADS server addresses. In response to this query, DNS-SD returns a list of AADS servers, any of which can be used for login.

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 Agent for Desktop 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 Agent for Desktop supports multiple PTR records. Avaya Agent for Desktop 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.

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 Agent for Desktop. 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*"

Chapter 8: Configuring reason codes

Reason Codes field descriptions

Avaya Agent for Desktop supports three classes of reason codes:

- Auxiliary
- Call Work
- Log Out

Avaya Aura® Communication Manager handles the reason codes as digit strings. With reason codes, you can associate comprehensive text strings to the digit strings for easy reference. The reason code represents the reason for not being at the workstation, call work related actions, or for not accepting the ACD call. The reason codes are displayed on the message window when an agent changes the work status to auxiliary or logs out from the ACD service.

By default, the system creates a default reason code each for Auxiliary and Log Out code types. You can change the default reason codes, but cannot delete the default reason codes. The default code is marked with a tick mark symbol (✓).

Using Avaya Aura® Communication Manager, you can now restrict an Avaya Agent for Desktop user from changing the Auxiliary reason code. The users receive an error when they try to change the Auxiliary reason code manually.

Name	Description
Menu items	The menu for selecting the list of reason codes to display. The reason codes that you can define are of the following types: • **Auxiliary Reason Codes**: The reasons for changing to the AUX state. • **Log Out Reason Codes**: The reasons for logging out from the ACD service. • **Call Work Codes**: The Call Work codes are the codes that user assigns to an active incoming ACD call from the call menu. The Call Work codes must be defined in the Settings window before using it. The Call Work codes can also be configured on ACM. To use the Call Work codes, extension must have 'work-code' feature button configured and 'Measured' parameter in Hunt Group settings must be set to 'both'. When you get an incoming ACD call, 'Add call work code' item is displayed in the call menu drop-down list. You can choose one of the work codes and add it to the call. If adding is successful, the selected code would be marked as checked in the list. You can add more than one work code to a call, but cannot add one code twice. Work codes can also be added through feature buttons window. Users have to click 'work-code' button and enter the work code (up to 8 digits). When a call is completed, added work codes are shown in the Call History window.
Locked	The reason codes received from ACM are marked with a lock icon in this column.
Default	A reason code marked as default cannot be deleted and always available for selection.
Reason Code	A field to define the display sequence of the reason codes. The reason code with value 0 is on the top followed by 1, 2, 3, etc.
Description	The text string that describes the reason code. This string is displayed on the top bar on selection.

Icon	Name	Description
	**Add Reason Code**	Add a new reason code to the list of reason codes.
	**Remove Reason Code**	Remove a reason code from the list of reason codes.

Functions of Aux Work Reason codes

Responses of Aux Work Reason codes to specific Communication Manager settings

The below functions are applicable only to Avaya Agent for Desktop registered in H.323 signaling mode:

- If Communication Manager feature-related system parameters 'Two-digit Aux Work Reason Codes' is 'No' and Avaya Agent for Desktop user enters two-digit code then Communication Manager accepts only the first digit without any error notification. If the user does not have Aux feature button configured with a corresponding resulting reason code, then the system may function in an expected way.
- Avaya Agent for Desktop setting in the server 'Local Server' settings is: "CM Forced type of Aux Reason Code Support Required". It is a checkbox setting and the checbox must be selected manually by the user when Communication Manager feature-related system parameters - Aux Work Reason Code Type is set to "Forced".
- When Avaya Agent for Desktop setting "CM Forced type of Aux Reason Code Support Required" is selected, the Aux Reason code 0 is not allowed to be used by the agent manually on UI level. Auxiliary 0 option is hidden in the main menu, 0 code is not accepted by Aux feature button.
- When Avaya Agent for Desktop setting "CM Forced type of Aux Reason Code Support Required" is selected, the user must set default reason code different from 0 (in Avaya Agent for Desktop settings - Reason codes - Auxiliary Reason codes).

Example

A user enters 12 as parameter for Aux Feature button without specifying a reason code. In this case, Communication Manager sets the code as 1 at the server side. If the user does not have Aux 1 button configured, Avaya Agent for Desktop shows 12 in the agent state notification area. Otherwise, if Aux 1 is configured then Avaya Agent for Desktop displays the correct Aux 1 state. This is because of an H.323 limitation that Communication Manager does not report any error during feature invocation. Also, Communication Manager cannot report any reason code back to Avaya Agent for Desktop if there is no corresponding feature button configured. So there is no possibility to track synchronization issues from Avaya Agent for Desktop (client) side.

- If Communication Manager feature-related system parameters "Two-digit Aux Work Reason Codes" and "Onhook Dialing on Terminals" are "Yes", and a user enters 1-digit Aux reason code, then the user needs to wait for about 10 seconds till Communication Manager accepts this code. As only one of two digits is entered, Communication Manager waits till dialing completes timeout before accepting the code. Enabling Normal feature button could be used as an indication that the operation is complete. The Normal button glows. Changing Aux code is not supported when the Normal button does not glow. Avaya Agent for Desktop must reflect correct state only when the Normal button glows.
- Onhook dialing setting must be in sync between Communication Manager and Avaya Agent for Desktop. If it is enabled on Communication Manager feature-related system parameters, then it must be enabled in Avaya Agent for Desktop settings also and vice versa. Other configuration variants are not supported.

Adding reason codes

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

Procedure

1. In the Avaya Agent for Desktop Settings window, click the **Reason Codes** tab.
2. In the left menu, select the reason code for which you want to add details. The options are:
   - **Auxiliary Reason Codes**: The reasons for changing to the AUX state.
   - **Log Out Reason Codes**: The reasons for logging out from the ACD service.
   - **Call Work Codes**: The Call Work codes are the codes that user assigns to an active incoming ACD call from the call menu. The Call Work codes must be defined in the Settings window before using it. The Call Work codes can also be configured on ACM. To use the Call Work codes, extension must have 'work-code' feature button configured and 'Measured' parameter in Hunt Group settings must be set to 'both'. When you get an incoming ACD call, 'Add call work code' item is displayed in the call menu drop-down list. You can choose one of the work codes and add it to the call. If adding is successful, the selected code would be marked as checked in the list. You can add more than one work code to a call, but cannot add one code twice. Work codes can also be added through feature buttons window. Users have to click 'work-code' button and enter the work code (up to 8 digits). When a call is completed, added work codes are shown in the Call History window.
3. Click ⊕.

Note:

The reason codes received from ACM are marked with a lock icon in the **Locked** column.

4. In the **Default** field, double-click in this column to mark a reason code as a default value.
5. In the **Reason Code** field, double-click the number and type the sequence number you want to associate with a reason code.
6. In the **Description** field, type the description of the reason code.
7. Click **Save**.

Removing reason codes

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

Procedure

1. In the Avaya Agent for Desktop Settings window, click the **Reason Codes** tab.
2. In the **Type** field, select the reason code type to display:
   - **Auxiliary Reason Codes**: The reasons for changing to the AUX state.
   - **Log Out Reason Codes**: The reasons for logging out from the ACD service.
   - **Call Work Codes**: The Call Work codes are the codes that user assigns to an active incoming ACD call from the call menu. The Call Work codes must be defined in the Settings window before using it. The Call Work codes can also be configured on ACM. To use the Call Work codes, extension must have 'work-code' feature button configured and 'Measured' parameter in Hunt Group settings must be set to 'both'. When you get an incoming ACD call, 'Add call work code' item is displayed in the call menu drop-down list. You can choose one of the work codes and add it to the call. If adding is successful, the selected code would be marked as checked in the list. You can add more than one work code to a call, but cannot add one code twice. Work codes can also be added through feature buttons window. Users have to click 'work-code' button and enter the work code (up to 8 digits). When a call is completed, added work codes are shown in the Call History window.
3. Click the reason code that you must remove.
4. Click the **–** button.
5. Click **Save**.

Chapter 9: Configuring greetings

Greetings tab field descriptions

In addition to recording an audio file, Avaya Agent for Desktop now provides option to upload multiple audio files for a greeting message. You can chose to activate a desired audio file from the list of audio files uploaded for a greeting message. You can also configure settings to auto-play the audio files based on the Avaya Agent for Desktop status. You can use the following descriptions from the **Greetings** tab to manage greetings.

Field	Description
Rule Name	The field to define the name of the new audio greeting rule.
VDN Name Pattern	The field to define the name of the new audio greeting rule in a regular expression format. For example – Special symbol *. VDN "Avaya*_VDN" will be triggered for "AvayaWeather_VDN", "Avaya123_VDN" and other VDN Names satisfy this rule. Special symbol ?. VDN "Avaya?VDN" will be trigerred for "Avaya1VDN", "Avaya2VDN" and similar.
Auto Play only if	The field to auto play the active audio file of a greeting message based on the status of the Avaya Agent for Desktop application. The following are the available options: • **Do not auto play**: The greeting message is not triggered and rule is disabled. • **For all incoming calls**: The greeting message is played for all incoming calls. The VDN expression is ignored. • **When agent is logged in**: The greeting message is played when agent is logged in irrespective of the agent state. The VDN expression is ignored. • **When agent is in Ready Mode**: The greeting message is played only when agent is in Ready state. Greeting message is played for all incoming calls if VDN is empty. If VDN is not empty, greetings which satisfy the VDN rule is played.

Table continues…

Field	Description
File name	The field to display and modify the file name of the active audio file.
File Path	The field to select an audio file.
Duration	This field displays the duration of the recorded audio greeting.
Recording	The field to record and play an audio file.

In addition to recording an audio file, Avaya Agent for Desktop now provides option to upload multiple audio files for a greeting message. You can chose to activate a desired audio file from the list of audio files uploaded for a greeting message. You can also configure settings to auto-play the audio files based on the Avaya Agent for Desktop status. You can use the following descriptions from the **Greetings** tab to manage greetings.

Note:

In Telecommuter mode for Avaya Agent for Desktop, greetings are not supported. The audio path is established between the TC device and the caller. In this case, Avaya Agent for Desktop does not participate in the audio transmission. This means that greetings configured on Avaya Agent for Desktop do not play on the caller side.

Adding a greeting message

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

About this task

You can configure the system to play a greeting message to the client when incoming calls are connected.

Procedure

1. In the Avaya Agent for Desktop Settings window, select the **Greetings** tab.
2. Click the **Add** icon in the left pane.
3. In the **Rule Name** field, type the name of the greeting message.
4. In he **VDN Name Pattern** field and type the name of the VDN associated to the greeting message.

   Note:

   When a call with an agent starts, the VDN name you define is displayed on the top bar. Also, the VDN name field can display only 16 characters (15 visible and 1 for string termination). Thus, if the VDN name is too long, then you must add a '*' to abbreviate.

The key point is that Avaya Agent will match the VDN name to play a greeting. For example, Queue to Virtual Agents must be added as Queue to*.

5. In the **Auto Play only if** field, click any one of the following options:
   - **Do not auto play**
   - **When agent is in Ready Mode**
   - **When agent is logged in**
   - **For all incoming calls**
6. **(Optional)** Click the **File Name** field, to modify the file name details.
7. **(Optional)** In the **File Path** field, click to select the required audio file.
8. In the **Recording** field, click **Record** to record a new audio message. Click **Stop** to stop recording.

   Note:

   The **Duration** field displays the duration of the recorded audio file and cannot be modified.
9. (Optional) Click the **Play** icon to listen to the recording.
10. To remove an audio file from the **Greetings List** , select an entry from the list and click the **Delete** icon.
11. Click **Yes** to confirm deletion.
12. Click **Save** to save the greeting message settings.

Removing a greeting message

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

Procedure

1. In the Avaya Agent for Desktop Settings window, click the **Greetings** tab.
2. Select the greeting in the left pane.
3. Click the delete icon.
4. Click **Yes** to confirm the deletion.
5. Click **Save**.

Changing the order of a greeting message

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Settings**. The system displays the Avaya Agent for Desktop Settings window.

Procedure

1. In the Avaya Agent for Desktop Settings window, click the **Greetings** tab.
2. Select the greeting in the left pane.
3. Click the up or down icon in the left pane to change the order of the greeting.
4. Click **Save**.

Chapter 10: Configuring screen pops

Screen pop tab field descriptions

You can configure Screen Pop for incoming and outgoing calls in Avaya Agent for Desktop. You can configure Screen pop to open a desktop application or a web service based on your requirement.

Name	Description
Rule name	The **Rule name** list displays a list of Screen Pops that you can use to open a program or a Web service.
Type	The field to specify whether you want to open an application or a web URL in an external or an internal browser. If you select Application, you need to locate and select the application in the **Application** field.
URL	Use this field to enter the URL of the Web program containing reference to a Web program and the call-related data in a Web program format. For example, to view the customer database program, in the **URL** field, type `http://internal.widgets.com/db/customers.exe`.

Table continues…

Name	Description
Parameters	Specify the parameters in the Parameter column. You can set the following parameters for the Screen pops: • <n> to pass the name of the other party on the call. • <m> to pass the phone number of the other party on the call. • <p> to pass the digits (prompted digits) the caller selected while processing through a vector. • <v> to pass the VDN name through which the call connects. • <u> to pass User-to-User-Information (UUI) that Communication Manager collects from a centralized application. **Note:** UUI length is limited to 32 bytes for H.323 stations. SIP stations support UUI length up to 128 bytes. • <s> to pass the time when Avaya Agent for Desktop accepts the call. • <e> to pass the time when Avaya Agent for Desktop ends the call. • <d> to pass the current date when Avaya Agent for Desktop receives the call. • <a> to pass the current AgentId. If agent is offline, then <a> parameter is skipped. • <i> to pass the current StationId. • <ucid> to pass the unique call id. • <vdntime> to pass the duration the call was on VDN call. This parameter is supported only in SIP mode. • <asai> to pass associated ASAI. This parameter is supported only in SIP mode.

Table continues…

Name	Description
Trigger	The field to indicate when the program must trigger the Screen Pop : • **Incoming call is ringing**: To open Screen Pop when the phone rings. • **Incoming call is answered**: To open Screen Pop when an agent answers the call using the Avaya Agent for Desktop GUI. • **Incoming call is missed**: To open Screen Pop when the call appearance from an incoming call disappears after no response and the caller hangs up. • **Incoming call is released**: To open Screen Pop when an incoming call is dropped or disconnected by an agent or a customer. • **Outgoing call is established**: To open Screen Pop when the called-party answers the phone. • **Outgoing call is released**: To open Screen Pop when an outgoing call is dropped or disconnected by an agent or a customer.
Trigger only for ACD calls	A field to trigger screen pop only when an ACD call arrives
VDN Name	When **Trigger only for ACD calls** is active, you need to define the VDN Name.

Icon	Name	Description
	**Add**	Add a new screen pop configuration.
	**Remove**	Remove a screen pop configuration from the list.

Creating a screen pop

About this task

You can configure a Screen Pop for incoming and outgoing calls and to open a desktop application or a web service.

For example, a client database, a trouble ticket application, a custom application to open a remote application containing reference to a web application, and other call-related data in a web program format.

Procedure

1. In the Avaya Agent for Desktop Settings window, click the **Screen Pop** tab.

   The system displays the Screen Pop screen.

2. In the **Screen Pop** left panel, click **Add** (⊕).

   The system displays an untitled item in the Screen Pop list.

3. In the **Rule Name** filed, click and rename the field name.

4. In the **Type** field, click one of the following :

   - **Application**: To browse and specify the path for an application on the local system. If you select Application, you need to locate and select the application in the **Application** field.
   - **External browser**: To specify the URL for a web service to open in an external browser.
   - **Internal browser**: To specify the URL for a web service to open in an internal browser.

5. In the **URL** field, do one of the following :

   - To open a remote application containing reference to a web application as a Screen Pop, type a valid web address.

     Note:

     The URL can be CGI scripts, Java scripts, or any other web-based tools. To view a URL on a telephone number parameter, the example must contain one of the Avaya Agent for Desktop (%) parameters as `http://mycompany.com/data?tel=%m`. The format of the URL depends on the data and format of the web program.

   - To use a Windows application as a screen pop, specify a valid directory path. For example, type `C:\Program Files\Adobe\Acrobat 7.0\Acrobat \Acrobat.exe`.

     Note:

     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 that is not specified in Windows Registry, the system displays an error message.

6. In the **Parameters** field, type the required parameter. .

7. To indicate when the application must trigger the Screen Pop, from **Trigger**, select the appropriate trigger.

8. To open a Screen Pop application for a specific VDN, select the **Trigger Only for ACD calls** check box and type the **VDN Name** in the corresponding field.

9. Click **Save**.

Chapter 11: Security

Overview

This chapter includes information about the following:

- Security requirements for Avaya Agent for Desktop
- Password storage encryption methods
- Security recommendations for desktop platform
- 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 Agent for Desktop allows 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`

Security requirements

Avaya recommends the use of TLS v1.2 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 Agent for Desktop can securely connect to network resources when using a secure server certificate obtained from a certificate authority.

To maintain a secure environment for Avaya Agent for Desktop, 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 Agent for Desktop. If you must use TCP for SIP connections, this cannot be configured by using the SIP server address in the client settings.

Avaya Agent for Desktop 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.

Before you begin

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:
    a. Clear the check box for Endpoint on TLS protocol.
    b. 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 Agent for Desktop 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/PKCS5P adding 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.

Port configuration

For information about the ports and protocols that Avaya Agent for Desktop uses, see the Avaya 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 Agent for Desktop 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 Agent for Desktop 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 Agent for Desktop 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 Agent for Desktop 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.

On Avaya Agent for Desktop for Windows, you can use the existing method, such as group policy, to install the client identity certificate on the OS.

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 "".

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® Session Manager
- Avaya Session Border Controller for Enterprise
- Web server, which you use to host the settings file for automatic configuration
- LDAP

Avaya Agent for Desktop 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 Agent for Desktop cannot establish a TLS connection because of an inability of the device to validate the certificate, Avaya Agent for Desktop displays an error message.

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 Agent for Desktop.
- An enterprise server certificate and if you already deployed the matching CA certificate to devices, you can continue to use Avaya Agent for Desktop.

Split-Horizon Domain Name System (DNS) scenario

For the TLS handshake between Avaya Agent for Desktop and Avaya SBCE, Avaya SBCE 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 Agent for Desktop and Avaya SBCE, the subject alternate name must be blank in the certificate that Avaya Agent for Desktop shares. For more information, see Administering Avaya Session Border Controller for Enterprise.

Certificate distribution

Avaya recommends the use of automatic configuration to distribute the CA certificates needed for Avaya Agent for Desktop.

The Avaya Aura® Device Services certificate must be available in the platform trust store. Avaya Agent for Desktop can then connect to Avaya Aura® Device Services 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 operating system.

Note:

Avaya Aura® Device Services is not used for H.323. Hence, Avaya recommends to select the certification mode as remote, and specify the patch to the configuration server.

Private trust store

The CA certificates can be hosted on the automatic configuration server to be distributed to Avaya Agent for Desktop. 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 Agent for Desktop uses the certificates in the private trust store for all operations.

  Hence, even if the certificates are locally available in the operating system, Avaya Agent for Desktop 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.

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 Agent for Desktop is used, you must:

- Keep OS components up-to-date.
- Use full disk encryption.
- Use anti-virus, anti-phishing, and other security tools.

No transference of sensitive data

Avaya recommends that there must be no transference of sensitive data through unprotected file sharing or mounted drives. Sensitive data, for example, Personally Identifiable Information (PII)

must not be transferred through unprotected file sharing or drive mounting mechanisms. Clear text NFS or SMB shares are not allowed.

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 Session Manager instance from the list.
3. In the **More Actions** field, click **Configure Trusted Certificates**.

   The system displays the 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. Perform one of the following:
   a. Upload the CA Certificate to a website and send your users the link.
   b. Send the CA certificate through email as an attachment.

Obtaining the Avaya Aura® System Manager CA certificate

Before you begin

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, in the Services area, click **Security** → **Certificates** → **Authority** → **CA Structure & CRLs**.
2. Click **Download pem file**.
3. Save the file to a location on your system.

4. Perform one of the following:
   - Upload the CA Certificate to a website and send your users the link.
   - Send the CA certificate through email as an attachment.

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 Agent for Desktop:

- Test Avaya Agent for Desktop prior to deployment. You must be able to install and start Avaya Agent for Desktop on a minimal machine, and be able to perform the following functions:
- Whitelist Avaya Agent for Desktop 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:
  - Minimum 1.6 GHz 32-bit or 64-bit CPU

    Test Avaya Agent for Desktop 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
  - 1.5 GB of free hard disk space
  - Keyboard
  - Mouse or other compatible pointing device
  - Headset for This Computer mode
- 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.

Supported cipher suites

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

Avaya Agent for Desktop supports the following cipher suites:

- TLS_RSA_WITH_AAES_128_SHA
- SSL_EDH_RSA_DES_64_CBC_SHA
- SSL_RSA_NULL_SHA
- TLS_RSA_WITH_NULL_SHA256
- TLS_RSA_WITH_AES_128_SHA256
- TLS_RSA_WITH_AES_256_SHA256
- TLS_DH_DSS_WITH_AES_128_SHA256
- TLS_DH_RSA_WITH_AES_128_SHA256
- TLS_DHE_DSS_WITH_AES_128_SHA256
- TLS_DHE_RSA_WITH_AES_128_SHA256
- TLS_DH_DSS_WITH_AES_256_SHA256
- TLS_DH_RSA_WITH_AES_256_SHA256
- TLS_DHE_DSS_WITH_AES_256_SHA256
- TLS_DHE_RSA_WITH_AES_256_SHA256
- TLS_ADH_WITH_AES_128_SHA256
- TLS_ADH_WITH_AES_256_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DH_RSA_WITH_AES_128_GCM_SHA256
- TLS_DH_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
- TLS_DH_DSS_WITH_AES_128_GCM_SHA256
- TLS_DH_DSS_WITH_AES_256_GCM_SHA384
- TLS_ADH_WITH_AES_128_GCM_SHA256
- TLS_ADH_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_SHA256

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 Agent for Desktop 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 Agent for Desktop 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 Agent for Desktop in the Guest mode with blacklisted ciphers because guest users do not have access to download the blacklisted cipher suites.

Chapter 12: 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 services packs are available. The Avaya Notifications process manages this proactive notification system.

Procedure

1. To sign up for notifications, go to http://support.avaya.com and search for “Avaya Support Web Tips and Troubleshooting: ENotifications Management”.
2. In the section **Results**, click **Avaya Support Web Tips and Troubleshooting: ENotifications Management**.
3. Set up e-notifications.

Viewing PCNs and PSNs

Procedure

1. Go to the Avaya Support website at https://support.avaya.com.

   If the Avaya Support website displays the login page, type your SSO login credentials.

2. At the top of the page, click **Support by Product** → **Documents**.
3. On the Documents page, in the **Enter Your Product Here** field, type the name of the product.
4. In the **Choose Release** section, select the specific release from the drop down list.
5. Select the appropriate filters as per your search requirement.

   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.

Appendix A: VLAN and 802.1 limitations on Windows 10

If you want to use QoS 802.1p tagging, you must enable it in Avaya Agent for Desktop. You need to set the value and Avaya Agent for Desktop will tag the packets by provided value. But in addition to it, the packet will be tagged by VLAN ID 0. So the network devices, such as switches and routers must be configured to pass the packets tagged by VLAN ID 0.

This is Avaya Agent for Desktop for Windows limitation. The reason for this limitation is that 802.1p label is part of 802.1q header of a network packet. So Avaya Agent for Desktop fill 802.1p by user provided value, but the other fields of 802.1q header are filled by the default value: VLAN ID = 0.

Appendix B: Data privacy controls

Personal data is stored on the file system that is accessible by the current user or a privileged user of the application. The file system content is not encrypted, but can be encrypted using platform technologies. When personal data is transmitted over a network, the data is encrypted with the latest protocols.

Data categories containing personal data

User data in memory:

- Remote-party phone number from calls
- Participant display name
- Contacts retrieved from the network
- Contacts retrieved from the network

User data on disk:

The following information is saved on the disk:

- Local call logs
- Agent’s information: Station ID and Agent ID

On Windows, the user’s credentials are saved in the Windows Credential Manager. in an area that is encrypted such that only the Windows user can decrypt not even the administrator. Users can access this area through Windows APIs.

On macOS, user’s credentials are saved in Keychain.

On Linux, the credentials are saved to Keyring.

If a secure storage is not available, the Station’s password, Agent ID’s password and/or Avaya Aura Control Manager ID’s password will be stored encrypted in the configuration file.

The user has the option not to enable saving of the passwords.

User data log:

The following information is saved:

- H.323 station number or SIP station number
- Display name information from SIP messages

The following information is not saved:

- Passwords

Personal data administrative controls

The administrator defines the file system access. The security best practices are to limit the file system access to any data store that contains personal information.

User data on disk:

Users can access the data by browsing through the file system on all supported operating systems.

User data logs:

Users can access the data logs:

- Through the file system on all supported operating systems
- By using the **Logs** > **Save as** option in Avaya Agent for Desktop client

Personal data programmatic or API access controls

User data in memory:

None

User data on disk:

Users can access the file system through the OS file system APIs.

User data logs:

Users can access the file system through the OS file system APIs.

Personal data “at rest” encryption controls

User data on disk:

The host platform can be configured to encrypt the file system content.

User data logs:

The host platform can be configured to encrypt the file system content.

Administrators must refer to the Operating System manual to enable file system encryption.

Personal data “in transit” encryption controls

HTTPS or TLS 1.2 sends or receives data with servers. This is implemented on all supported platforms.

The Remote logging option is turned off by default and it can be set up with TLS if required. External applications interfacing with CTI are not in scope of Avaya Agent for Desktop.

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 the 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 the disk is permanent, whether application is reset or uninstalled, until the user manually deletes the data from the file system.

User data logs:

Log data is stored until log files are rolled over. Roll over is set by file size and log files can also be manually deleted. You must refer to the section '*Deleting the log files manually*' of this guide to delete the files.

Personal data export controls and procedures

User data in memory:

Not applicable

User data on disk:

Users or administrators can access the user data on disk. Local configuration, call log, and log files can be copied to an external system.

User data logs:

Log files can be copied to an external system. The **Logs** > **Save as** option can be selected to compress and save the log files into the destination the user chooses.

Personal data view, modify, delete controls and procedures

User data in memory:

Not applicable

User data on disk:

The user and administrator have access to the file system. The user can also edit configuration data and local contact's list in the application's interface. User can also delete call log information from the application's interface.

User data logs:

The administrator and the user have full read or write access to the file system where the logs are stored.

Personal data pseudonymization operations statement

User data in memory:

None

User data on disk:

None

User data logs:

None

Appendix C: Configuring Avaya Session Border Controller for Enterprise for Avaya Aura® Remote Worker

Remote worker overview

Avaya Session Border Controller for Enterprise (SBCE) delivers security to a SIP-based enterprise network. This section provides details on how to configure Avaya SBCE for Avaya Aura® Remote Worker. The remote worker feature supports SIP deployments and extends access to the features of an internal enterprise Unified Communications (UC) and Call Center (CC) network. Therefore, a remote worker can also be a CC agent (Avaya Agent for Desktop agent). The extended features include firewall or Network Address Translation (NAT) traversal, encryption, user authentication, and enforcement of session-endpoint call policies.

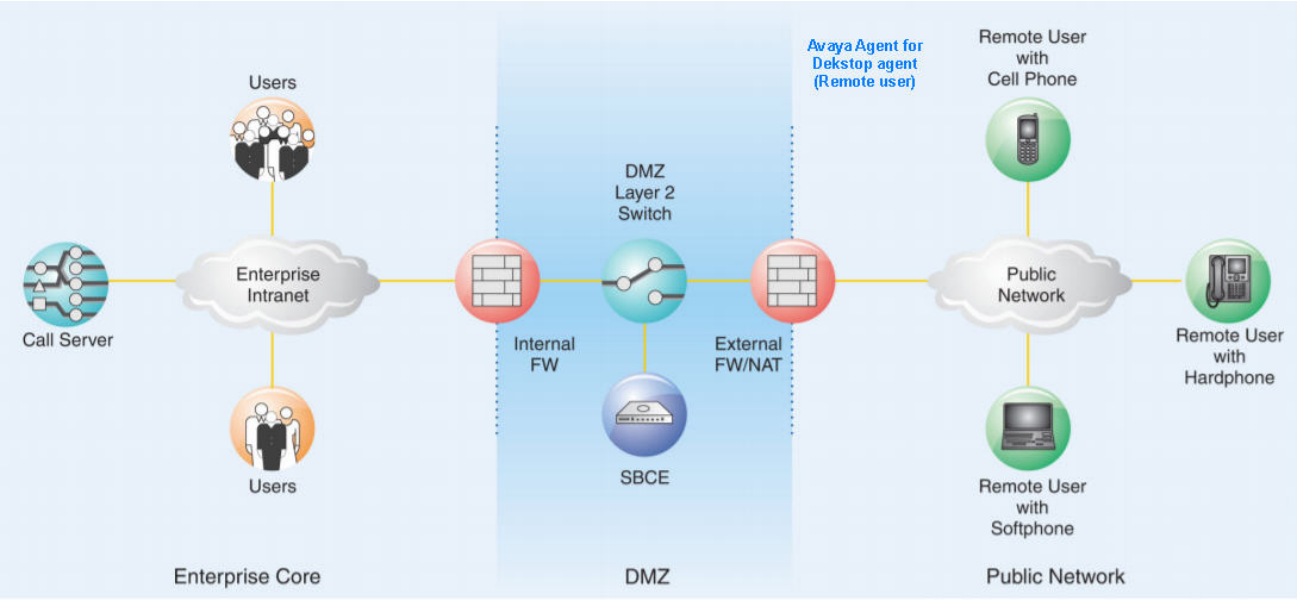


Figure 16:

For more details, see Chapter 12: Configuring Avaya Session Border Controller for Enterprise for Avaya Aura® Remote Worker of *Administering Avaya Session Border Controller for Enterprise guide, Release 8.1, Issue 2* located on the Avaya support site.

Glossary

After Call Work	An agent state consisting of work related to the preceding Automatic Call Distribution (ACD) call.
Automatic Call Distribution	A programmable device at the contact center. Automatic Call Distribution (ACD) handles and routes voice communications to queues and available agents. ACD also provides management information that can be used to determine the operational efficiency of the contact center.
Aux	The Aux or Auxiliary message indicates that the agent is not ready for ACD calls. However, agents can make or receive calls on the station while in the Aux state.
Avaya Agent	Avaya Agent for Desktopis a client application for a contact center agent, whichAvaya Agent for Desktop supports multiple OS platforms and use cases, such as VDI and standalone deployments.
Avaya Aura® Communication Manager (CM)	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.
Avaya Control Manager	Avaya Control Manager is a centralized operational administration solution that enables contact center administrators and supervisors to control all of the administrative elements that comprise a single or multiple location Avaya-based contact center environment. Contact center users, agents and other entities can be managed from a single Web-based user interface and provisioned across a range of Avaya applications in a contact center environment.
File Transfer Protocol (FTP)	An Internet protocol standard that is used to copy files from one computer to another.
HP Device Manager (HPDM)	HP Device Manager is a server-based application that provides sophisticated centralized administration capabilities for Thin Client devices running HP software.

Lightweight Directory Access Protocol (LDAP)	A set of protocols for accessing information directories. LDAP is based on X.500 standards, but it is simpler and supports TCP/IP for Internet access. Thus, it has become the standard for Internet-based applications. The Internet Messaging feature uses LDAP to provide access to an Internet directory from certain email products.
Local Area Network (LAN)	A network of personal computers that communicate with each other and that normally share the resources of one or more servers.
Log Out	To log out of the Avaya Agent for Desktop station and change the agent state to offline mode.
Random Access Memory (RAM)	The memory used in most computers to store the results of ongoing work and to provide space to store the operating system and applications that are actually running at any given moment.
Uniform Resource Locator (URL)	An Internet text address stored in a format recognized to signify a link. A uniform resource locator is a standardized way of representing different documents, media, and network services on the World Wide Web.
VDI	Avaya Virtual Desktop Infrastructure (VDI) is a product developed for enabling desktop virtualization, encompassing the hardware and software systems required to support the virtualized environment. Avaya Virtual Desktop Infrastructure is designed to function with: • The VDI Virtual Machine: A virtualized server for accessing the call handling features remotely. • The VDI Thin Client: A hardware device that has minimal system requirements and is used for hosting the VDI Client software.
Voice over Internet Protocol (VoIP)	A set of facilities that use the Internet Protocol (IP) to manage the delivery of voice information. In general, VoIP means to send voice information in digital form in discrete packets instead of in the traditional circuit-committed protocols of the public switched telephone network (PSTN).
Wide Area Network (WAN)	A data network typically extending a local area network (LAN) over telephone lines to link with LANs in other buildings and/or geographic locations.
Wyse Device Manager (WDM)	Wyse Device Manager (WDM) offers powerful and secure management software to configure, update, and administer Dell Wyse endpoint devices.

Index

A

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W