Deploying and configuring Avaya Agent for Desktop

Release 1.7.2
May 2018

© 2014-2018, Avaya Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

“Documentation” means information published 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. 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. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction 6
Purpose 6
Intended audience 6
Related Resources 6
Documentation 6
Chapter 2: Overview 8
Avaya Agent for Desktop overview 8
New in this release 14
Chapter 3: Topology 16
Hardware requirements 19
Software requirements 19
Network requirements 21
Port requirements 22
WebLM requirements 23
Audio requirements 24
Interoperability 26
Chapter 4: Deployment process 28
Chapter 5: Installation and configuration 29
Installation checklist 29
Obtaining the Avaya Agent for Desktop installer 29
Configuring the FTP server for a Linux thin client for VDI deployment 31
Configuring the FTP server for a Windows thin client for VDI deployment 32
Installing Avaya Agent for VDI through FTP server 33
Installing Avaya Agent for VDI remotely 36
Installing Avaya Agent for Desktop as a standalone Windows application 42
Installing Avaya Agent for Desktop as a standalone Mac application 44
Installing Avaya Agent for Desktop for a headless mode 46
Performing silent installation of Avaya Agent for Desktop 48
Assigning functions to buttons in Avaya Aura® Communication Manager 49
Assigning functions to buttons for SIP users in Avaya Aura® System Manager 50
Configuring Avaya Agent using the Configuration menu 51
Familiarizing with the Avaya Agent user interface 51
Configuring the connection to Avaya Control Manager 71
Configuring the WebLM license URL for H.323 and SIP 72
Configuring the connection to Avaya Aura® Communication Manager 73
Configuring the connection to a SIP proxy server 74
SIP shared control mode overview 75
Configuring the directory settings for H.323 and SIP 77
Configuring the dialing rules 78

Enabling the auto answer feature..... 79
Enabling the drop call button..... 80
Configuring the ready mode option..... 80
Configuring the after call work settings..... 81
Configuring the login and interface settings..... 81
Configuring the Login mode settings..... 82
Avaya Agent for Desktop supervisor feature overview..... 82
Configuring the transfer and the conference types..... 84
Message waiting indicator overview..... 85
Configuring the startup message..... 86
Adding reason codes..... 87
Removing reason codes..... 87
Configuring the audio input..... 88
Configuring the audio output..... 88
Configuring the ringer output..... 89
Configuring the advanced audio settings..... 89
Adding a greeting message..... 90
Removing a greeting message..... 91
Changing the order of a greeting message..... 91
Creating a screen pop..... 92
Setting the language for Avaya Agent for Desktop..... 93
Configuring logs..... 94
Configuring the RTCP Monitoring Server settings..... 95
Configuring QoS tagging for audio..... 95
Configuring QoS tagging for signals..... 96
Configuring the password storage settings..... 96
Changing the user password using Config.xml file..... 96
Configuring the PPM Secure Mode settings..... 97
Configuring the security settings..... 97
Configuring the SRTP settings..... 97
Avaya Agent for Desktop Presence feature overview..... 98
Commonly used Signalling DSCP values..... 100
Lock Manager overview..... 101
Breeze integration and feature support..... 110
Glossary..... 112

Chapter 1: Introduction

Purpose

This document describes how to install, configure, and uninstall the product.

Intended audience

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

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
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
Administering Avaya Aura® Call Center Elite	Provides information about administering Automatic Call Distribution (ACD) and Call Vectoring features.	Implementation engineers and system administrators.
Avaya Application Solutions: IP Telephony Deployment Guide	Provides information about Avaya's Application Solutions product line, IP Telephony product deployment, and	Implementation engineers, support personnel, sales

Table continues…

Title	Description	Audience
	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.	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

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 based operating systems WES7 and WES8 and Linux based operating systems Debian Linux and SUSE Linux primarily running on HP and Dell Wyse respectively. 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 7, Windows 10, WES-8, and Apple Mac.

  Note:

  A new client software has also been designed for Apple Mac for use on the following versions: Mavericks 10.9, Yosemite 10.10, El Capitan 10.11, and Sierra 10.12. This new software, called Avaya Agent for Desktop for Mac, is specifically developed for contact centers using Mac platform and supports both H.323 and SIP signaling protocols.

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.

Usage scenarios

The following diagrams depict the various methods of using the Avaya Agent for Desktop application:

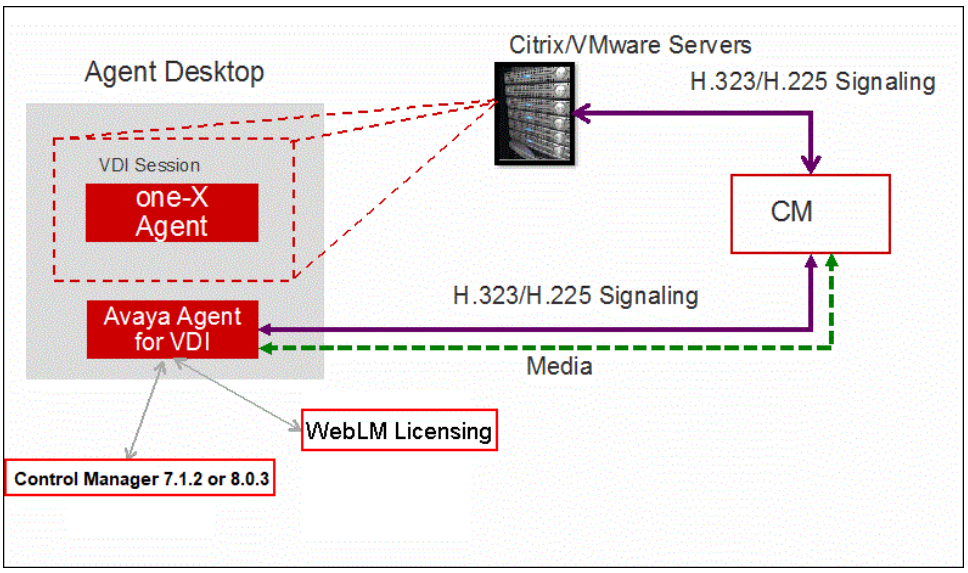


Figure 1: VDI solution with H.323

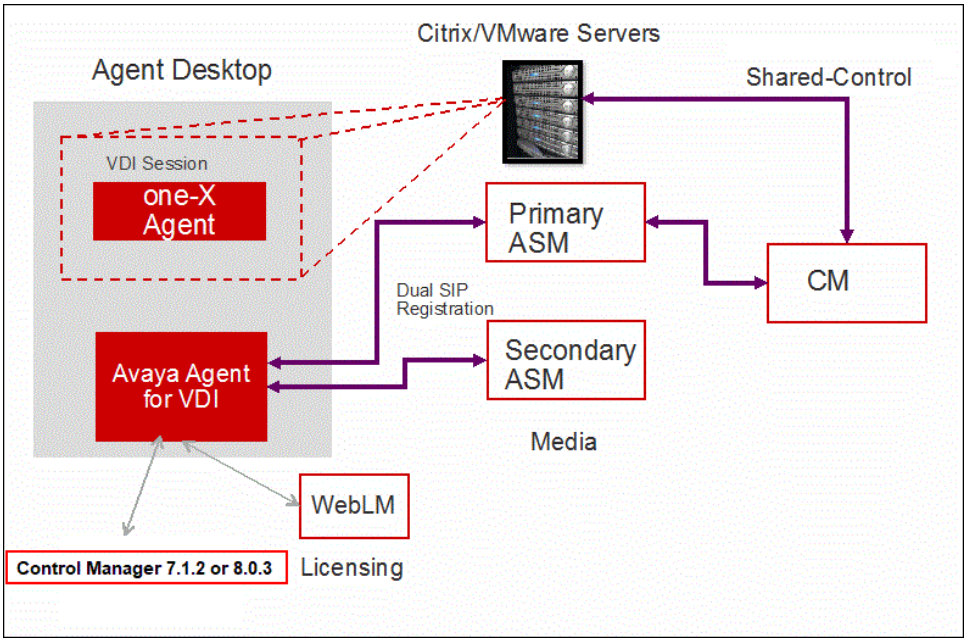


Figure 2: VDI solution with SIP

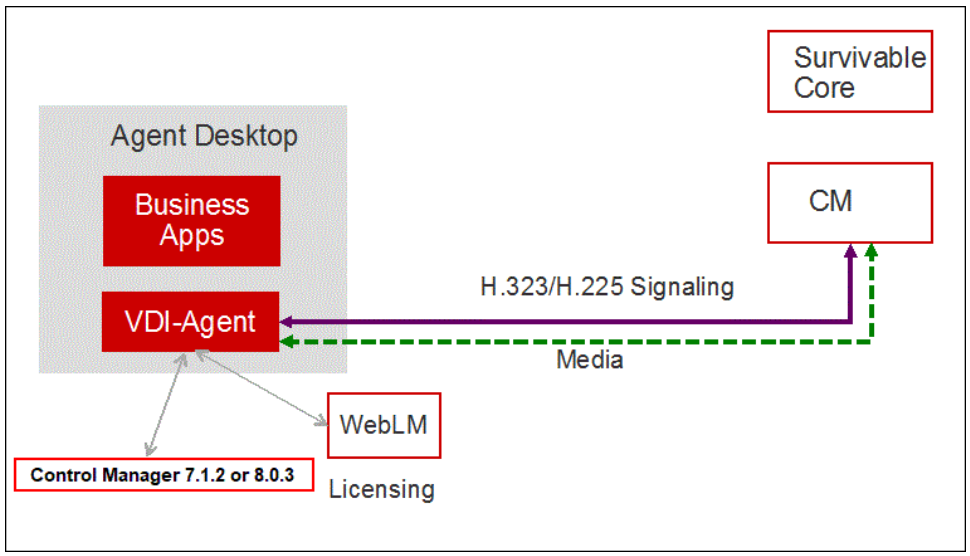


Figure 3: Standalone solution for H.323

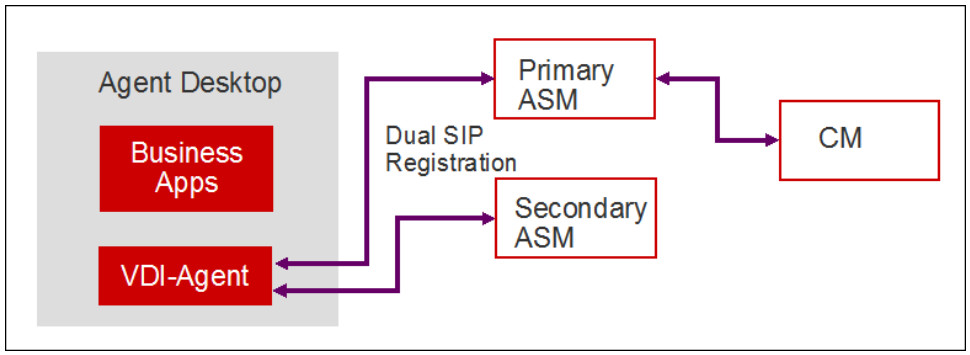


Figure 4: Standalone solution for SIP

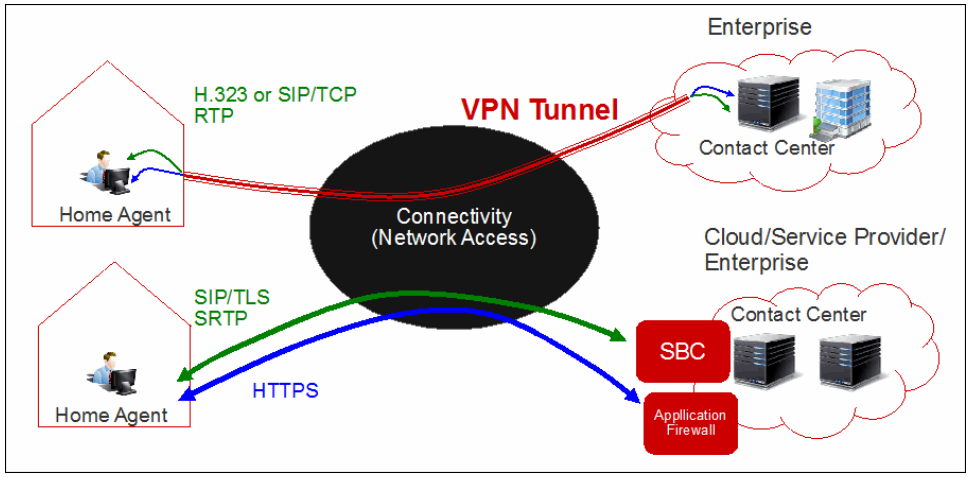


Figure 5: Remote agent solution for both VPN and SBC

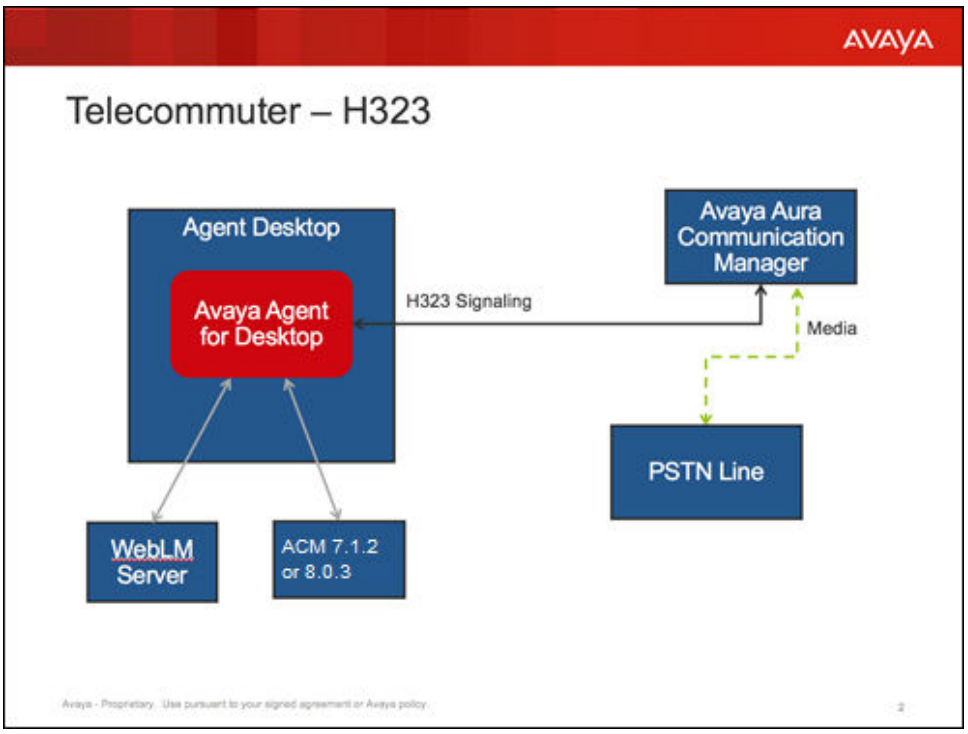


Figure 6: Telecommuter mode with H.323

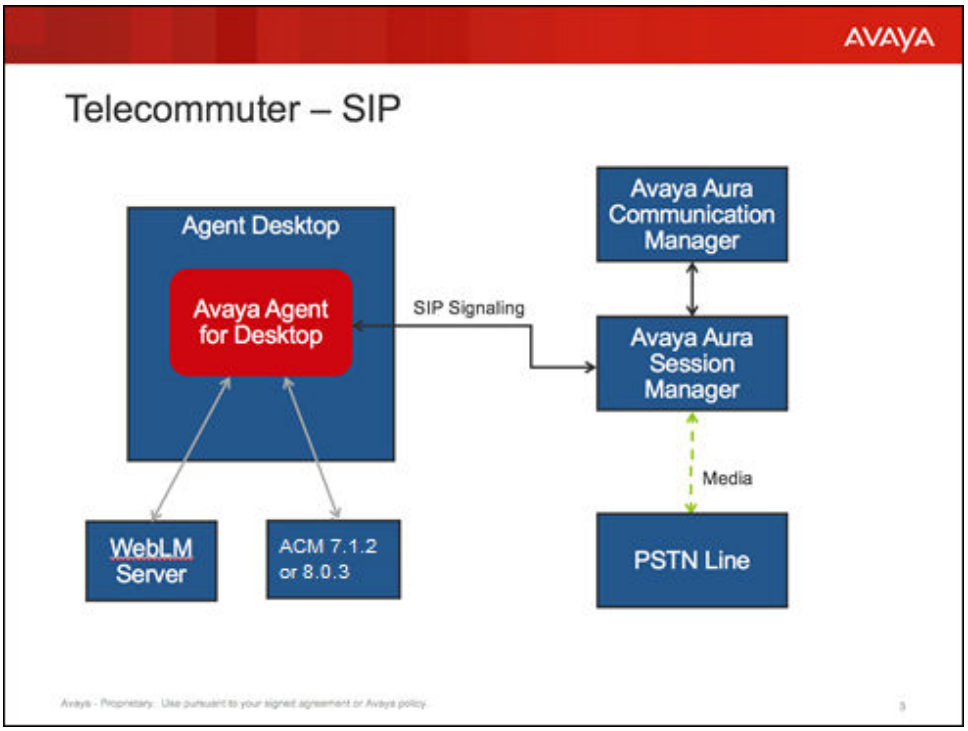


Figure 7: Telecommuter mode with SIP

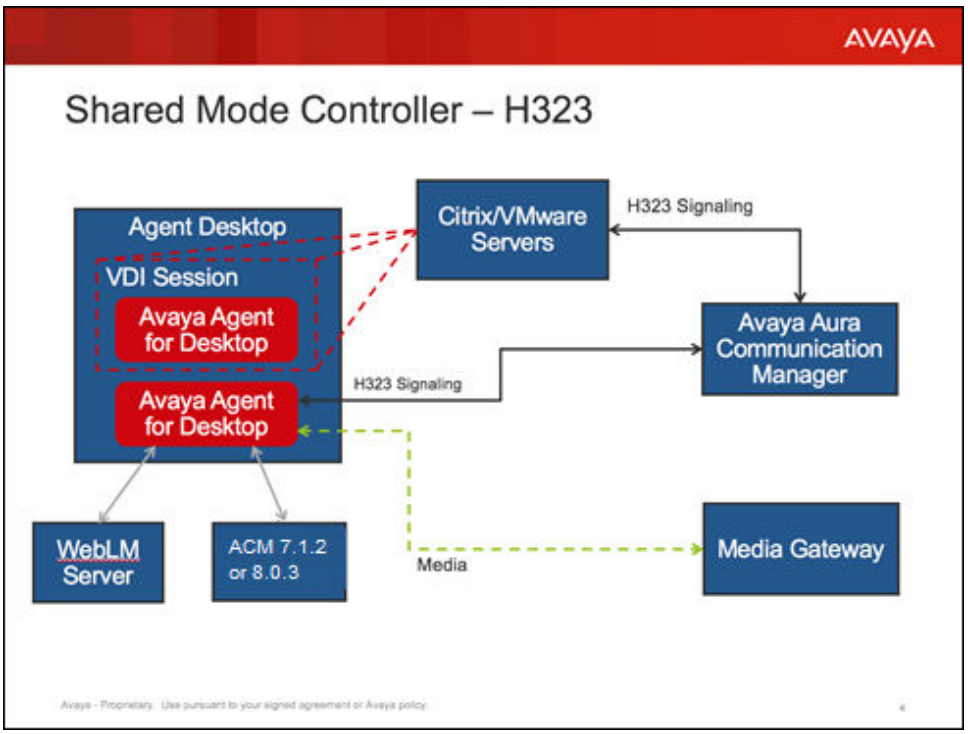


Figure 8: Shared Control as Controller with H.323

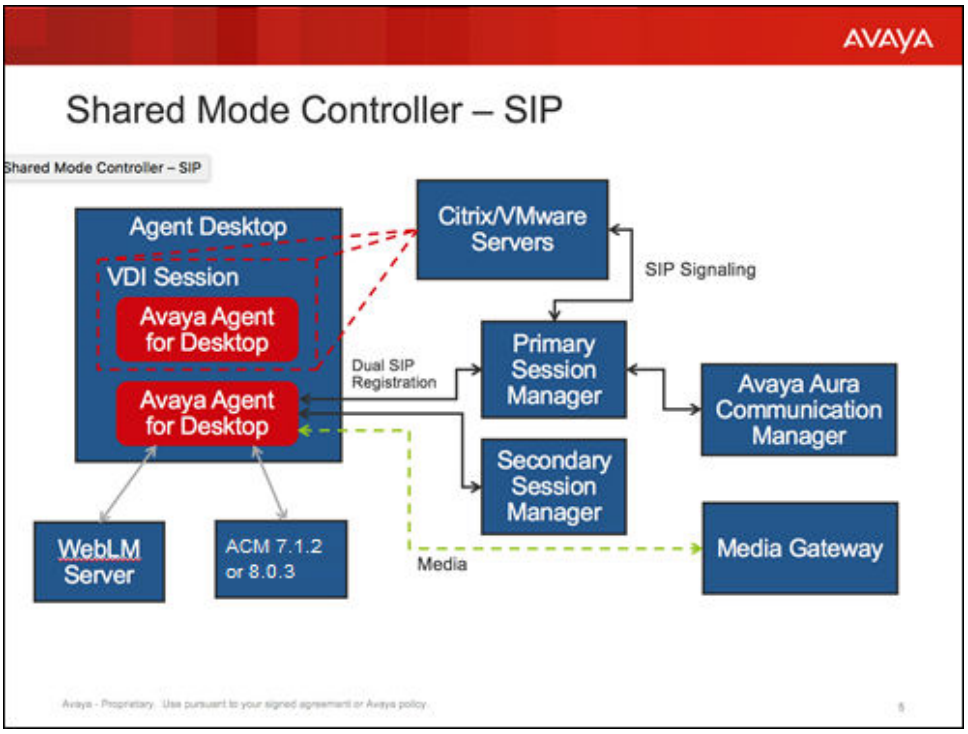


Figure 9: Shared Control as Controller with SIP

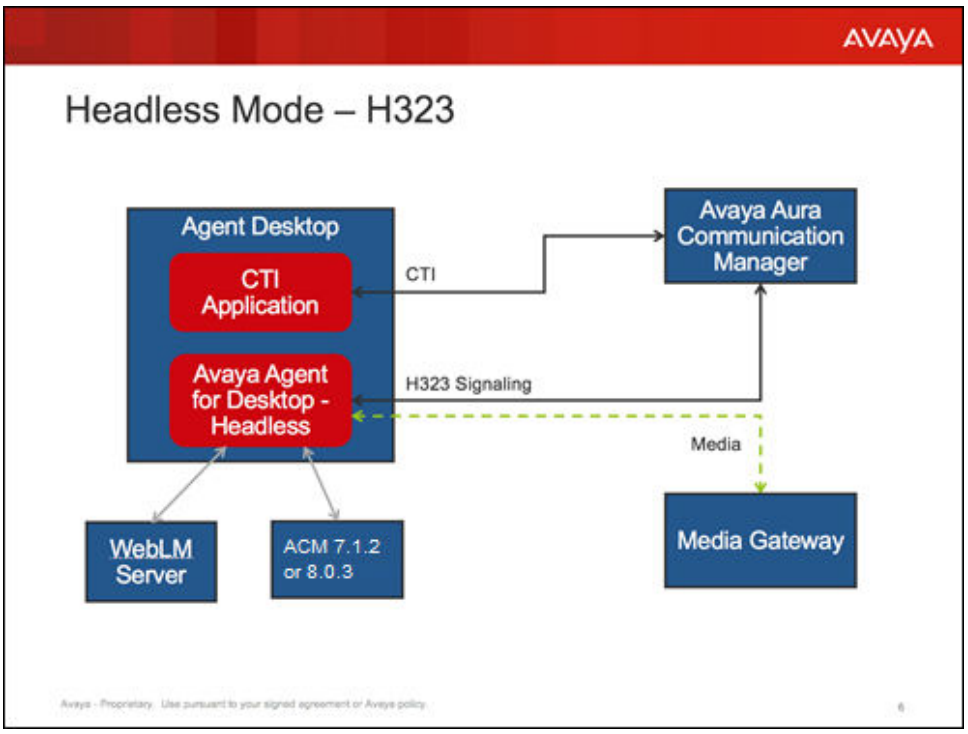


Figure 10: Headless Mode – H.323

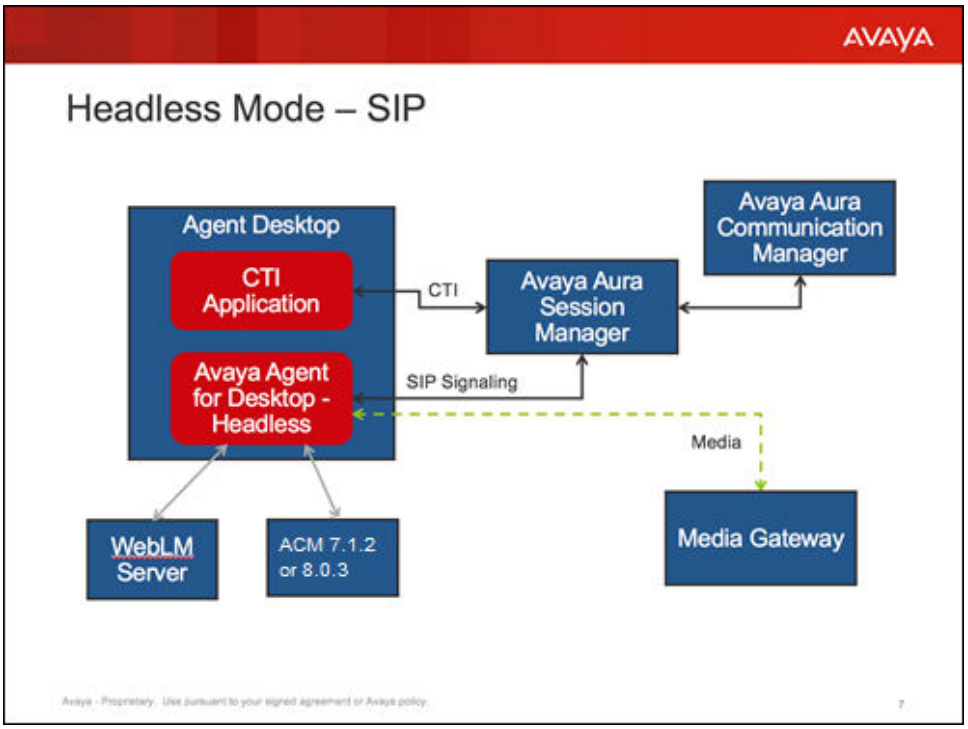


Figure 11: Headless Mode – SIP

New in this release

- **Station type support enhancement**: Avaya Agent for Desktop now supports the following station types:
  - For H.323: 9650
  - For SIP: 9650 SIPCC
- **Forced AUX reason code support**: Using Avaya Aura® Communication Manager, you can now restrict an Avaya Agent for Desktop user from changing the AUX reason code. The users will receive an error when they try to change the AUX reason code manually.
- **New log files support**: 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.
- **Enhanced support to change a local user's password using the Config.xml file**: You can now change the Avaya Agent for Desktop's local user password using the `Config.xml` file. To use the password from `Config.xml` file and not from Security Storage, you need to activate the UsePSWDFromConfigFile parameter in the `Config.xml` file.
- **Set storage limit of log files**: Using Avaya Agent for Desktop, you can now 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.
- **Call work reason code support**: Using Avaya Agent for Desktop, you can now allow agents to select call work reason codes. This functionality works during an active ACD call only. The system also stores the Call Work reason code related logs in the new Call History column (Work Codes).
- **Support to add a call drop button on the call appearance section**: Using Avaya Agent for Desktop, you can now allow users to add a call drop button up-front on the call appearance section. You can enable or disable this option using the Configuration settings window.
- **Support to control a local Avaya Agent for Desktop mute button from a mute button in a VDI session**: The mute button on Avaya Agent for Desktop instance in Desk Phone mode can now control and mute or unmute the microphone of Avaya Agent for Desktop instance in the local session in My Computer mode. This functionality works only in SIP mode.
- **Support for multiple ACM login types**: You can now use three different types of ACM login options to log in to Avaya Agent for Desktop. The options are:
  - **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.
  - **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.

  - **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.

- **Extension support on Google Chrome 65 and above version only**: Avaya Agent for Desktop browser extension is now supported on Google Chrome 65 and above version only.
- **Support to select UI language on EULA welcome screen**: Administrators can now select the default UI language on EULA welcome page itself while installing Avaya Agent for Desktop. Once the default language is selected, all screens after the selection is displayed in the selected language only.

Chapter 3: Topology

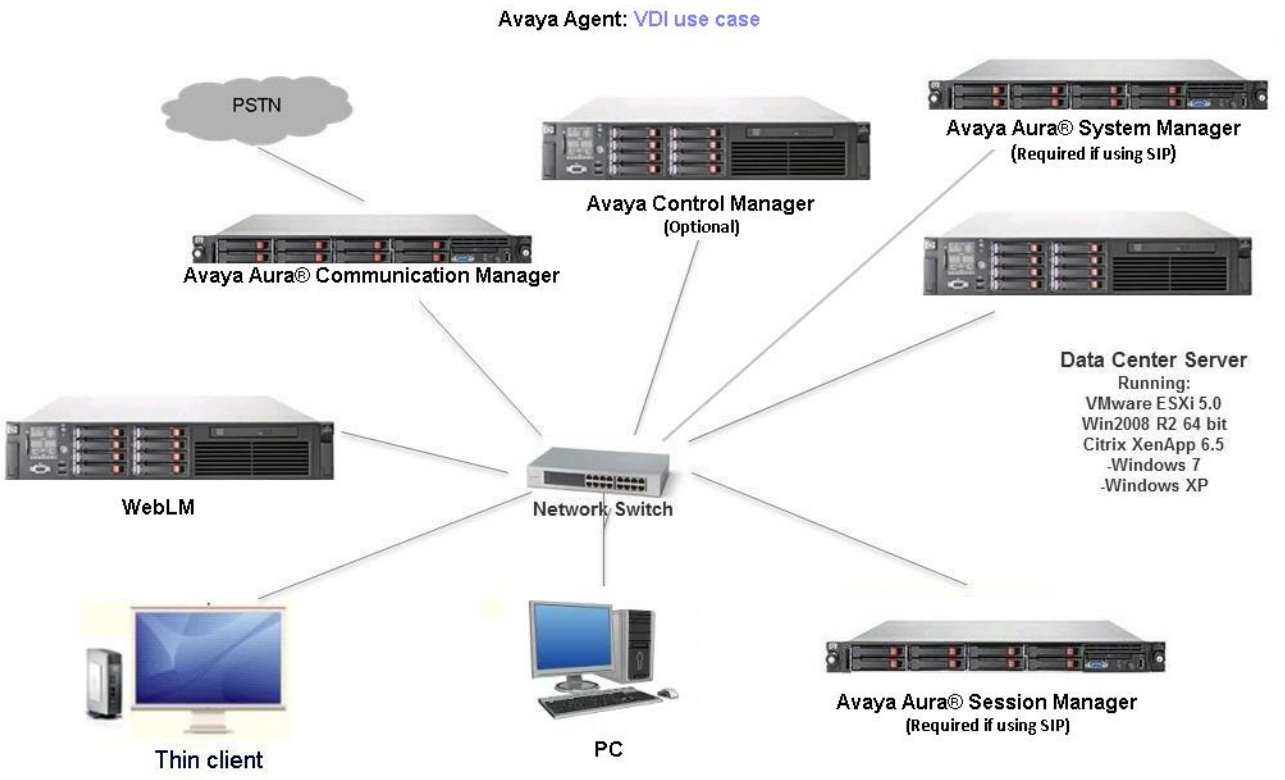


Figure 12: Avaya Agent for Desktop topology diagram: VDIA use case

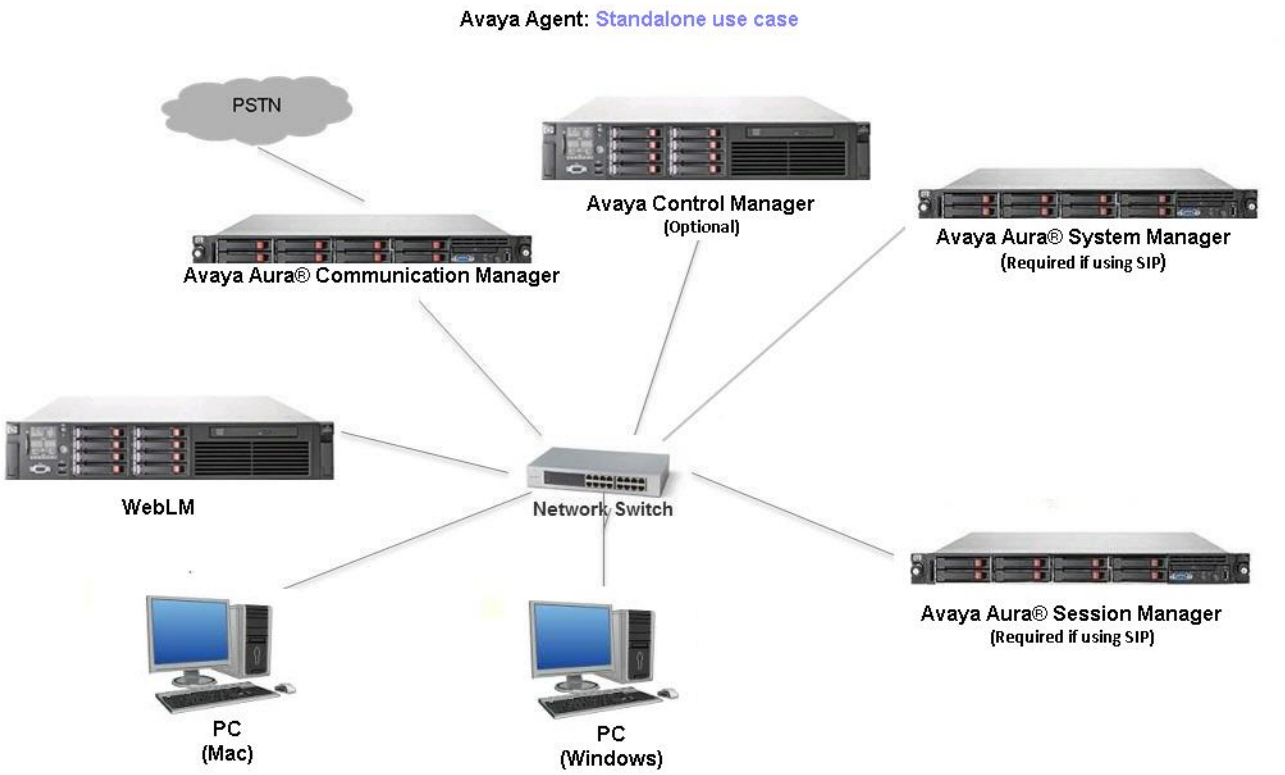


Figure 13: Avaya Agent for Desktop topology diagram: Standalone use case

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.
Avaya Aura® System Manager	Avaya Aura® System Manager is a central management system that provides a set of shared

Table continues…

Component	Description
	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.
Thin client	The thin clients where Avaya Agent for Desktop is deployed. **Warning:** If a customer installsAvaya Agent for Desktop in the environment other than the following mentioned environments, the system may experience some unexpected behavior. The thin clients that are currently supported are: • Dell Wyse D90D7 (WES7) • Dell Wyse Z50D (SUSE Linux) • HP T510 (WES7) • HP T520 (WES7) • HP T610 ThinPro (Debian Linux) • HP T610 (WES7) • HP T620 (WES8)
Data Center Server	The virtualization server that hosts the PC capabilities of the thin clients.

Related links

Hardware requirements on page 19
Software requirements on page 19
Network requirements on page 21
Port requirements on page 22
WebLM requirements on page 23
Audio requirements on page 24

Interoperability on page 26

Hardware requirements

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

- Dell Wyse clients: Wyse Z50D and Wyse D90D7.
- HP thin clients: HP ThinPro 610 (Debian Linux), HP 510, HP 520 WES7, and HP 620 WES8.

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
- RAM: 1 GB or higher
- Mac with Yosemite 10.10, EL Capitan 10.11, Sierra 10.12, and High Sierra 10.13 is available on all supported Mac hardware

Avaya Agent for Desktop supports the following station types:

- For H.323: 9650, 4620, 9640, 9641, 9608, 9621, and 9611.
- For SIP: 9650 SIPCC, 9608 SIPCC, 9641 SIPCC, 9621 SIPCC, and 9611 SIPCC.

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.

Related links

Topology on page 16

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 7 Professional
- Microsoft Windows 8.1
- Microsoft Windows 10

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:

- HP ThinPro Linux: Supports only 5.0, 5.1, and 5.2
- Apple OS X: Supports Mavericks 10.9, Yoesemite 10.10, El Capitan 10.11, Sierra 10.12, and High Sierra 10.13
- Ubuntu 12.0 (32-bit)

Browser Requirements

Table 2:

Operating Systems/ Browsers	Windows	Mac OS	Linux openSuse11	Linux thinpro
Embedded browser	Supported	Supported	Supported	Supported
Google Chrome version 65 or above	Supported	Supported	Not supported	Not supported
Mozilla Firefox	Supported	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

Related links

Topology on page 16

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 will 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.

For more information about network assessments, please consult:

- *"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://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*.

Related links

Topology on page 16

Port requirements

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	
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	

Table continues…

Source		Destination		Network or Application protocol	Traffic purpose	Comment
Initiator	Ports	Receiver	Ports			
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.
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)	

Related links

Topology on page 16

WebLM requirements

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

Related links

Topology on page 16

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.

Supported headsets:

Table 3: Supported headsets for Avaya Agent for Desktop

Headset	Adapter	Available features
Plantronics Encore Pro HW291N	Plantronics DA-60 Adaptor	• Increase volume • Decrease volume
Plantronics C310	NA	• Increase volume • Decrease volume • Mute / Unmute
Plantronics C320	NA	• Increase volume • Decrease volume • Mute / Unmute
Plantronics C510	NA	• Increase volume

Table continues…

		• Decrease volume • Mute / Unmute
Plantronics C620	NA	• Increase volume • Decrease volume • Mute / Unmute
Plantronics DA60	NA	• Increase volume • Decrease volume • Mute / Unmute
Jabra GN2000 Duo Noise Canceling IP	Jabra Link 220 Adaptor	NA
Jabra GN2000 Duo Noise Canceling IP	Jabra LINK 280 Adaptor	• Increase volume • Decrease volume • Mute / Unmute
Jabra biz 2300 USB mono	NA	• Increase volume • Decrease volume • Mute / Unmute
ENCORE PRO HW301N	DA45	• Increase volume • Decrease volume • Mute / Unmute

Fully supported headsets:

- Plantronics Blackwire 315.1
- Plantronics 510
- Plantronics Blackwire C220 M
- Plantronics C610
- Jabra EVOLVE 40 LINK
- Jabra Biz 2400 II CC
- Jabra Biz 2300

Only input supported headsets:

- Plantronics Blackwire C310
- Plantronics C520

Fully supported adapters:

- Plantronics DA80
- Plantronics DA90

Only input 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.

Related links

Topology on page 16

Interoperability

Aura 6.x interoperability

Avaya components	Supported release
Avaya Aura® Communication Manager	6.3.13 (SP3)
Avaya Aura® Session Manager	6.3.16.0.631601
Avaya Aura® System Manager	6.3.16
Avaya Aura® Messaging	6.3.53.0
Avaya Control Manager	7.1.2 or 8.0.3
Avaya Aura® Application Enablement Services	6.3.3 Patch 5
Avaya Session Border Controller for Enterprise	6.3 SP5
Avaya Contact recorder	15.1
Avaya WebLM Server	7.0.1

Aura 7.0 interoperability

Avaya components	Supported release
Avaya Aura® Communication Manager	7.0.0.2.0-SP2 or 7.0.1.2.0.441.23523
Avaya Aura® Session Manager	7.0.0.1.700102 or 7.0.1.1.701114
Avaya Aura® System Manager	7.0.0.1 or 7.0.0.0.16266
Avaya Aura® Messaging	6.3.53.0
Avaya Control Manager	7.1.2 or 8.0.3
Avaya Aura® Application Enablement Services	7.0.1.0.0.15-0
Avaya Session Border Controller for Enterprise	7.0.0.21
Avaya Contact recorder	15.1
Avaya WebLM Server	7.0.1

Aura 7.0.1 interoperability

Avaya components	Supported release
Avaya Aura® Communication Manager	7.0.1.1
Avaya Aura® Session Manager	7.0.1.1
Avaya Aura® System Manager	7.0.1
Avaya Aura® Messaging	6.3.3 SP5
Avaya Control Manager	7.1.2 or 8.0.3
Avaya Aura® Application Enablement Services	7.0.1
Avaya Session Border Controller for Enterprise	7.1
Avaya Contact recorder	15.1
Avaya WebLM Server	7.0.1

Aura 7.1 interoperability

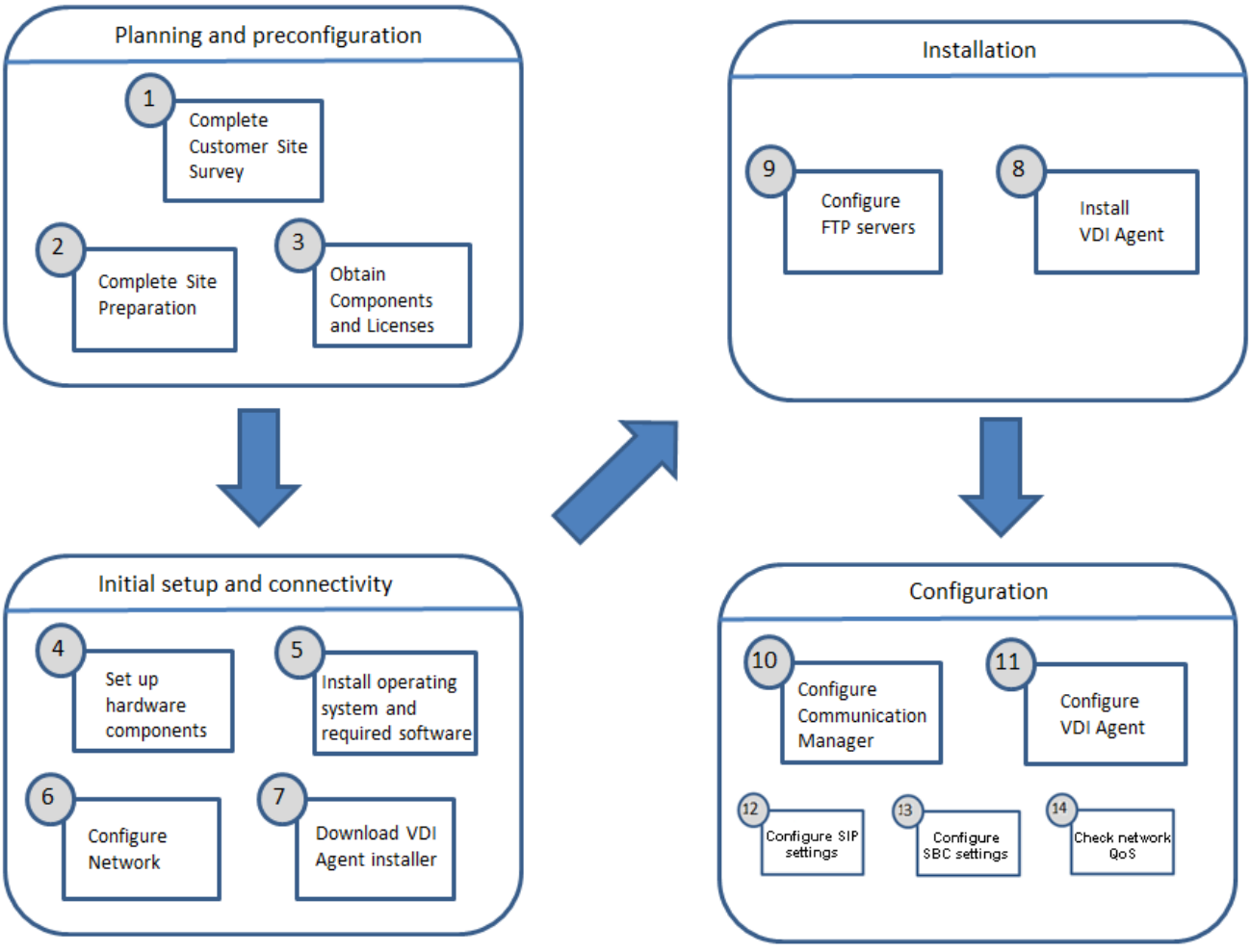
Avaya components	Supported release
Avaya Aura® Communication Manager	7.1.0.0.532
Avaya Aura® Session Manager	7.1.0.0.710028
Avaya Aura® System Manager	7.1.0.0.1125193
Avaya Aura® Messaging	7.0
Avaya Control Manager	7.1.2 or 8.0.3
Avaya Aura® Application Enablement Services	7.1.0.0.0.17
Avaya Aura® Presence Services	7.0

Related links

Topology on page 16

Chapter 4: Deployment process

The following image provides an overview of the Avaya Agent for Desktop deployment process.



Chapter 5: Installation and configuration

Installation checklist

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 29
Configuring the FTP server for a Linux thin client for VDI deployment on page 31
Configuring the FTP server for a Windows thin client for VDI deployment on page 32

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 and with the .rpm or .deb extension for Linux systems. The Mac version is delivered via .zip file.

If you deploy Avaya Agent for Desktop on Dell Wyse bricks, you must select the .rpm file that is required for the version of the operating system present on the brick:

- For SLETC 11 SP1, the name of the installer is `avaya-agent-<release_number>.sletc11sp1.rpm`
- For SLETC 11 SP2, the name of the installer is `avaya-agent-<release_number>.sletc11sp2.rpm`

Related links

Installation checklist on page 29
Downloading software from PLDS on page 30

Downloading software from PLDS

About this task

Note:

You can download product software from http://support.avaya.com also.

Procedure

1. Type http://plds.avaya.com in your Web browser to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS website.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Search for the available downloads using one of the following methods:
   - By download name
   - By selecting an application type from the drop-down list
   - By download type

   After entering the search criteria, click **Search Downloads**.
6. Click the download icon from the appropriate download.
7. When the system displays the confirmation box, select **Click to download your file now**.
8. If you receive an error message, click the message, install Active X, and continue with the download.
9. 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 29

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:

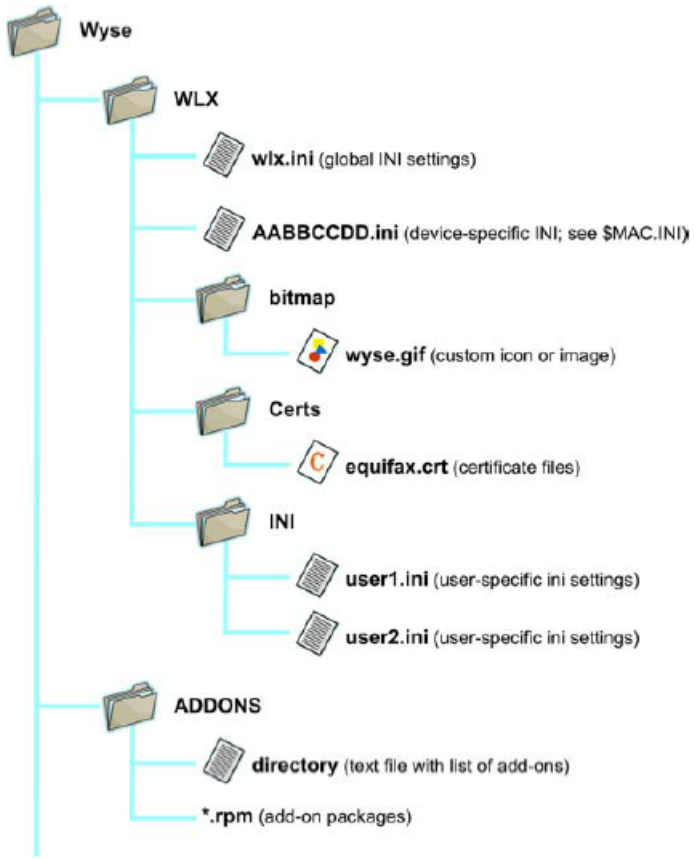


Figure 14: Wyse directory structure

Related links

[Installation checklist](#) on page 29

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.

Related links

Installation checklist on page 29

Installing Avaya Agent for VDI through FTP server

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

About this task

The following procedure describes the steps to install Avaya Agent for Desktop on the following Suse Linux-based Dell Wyse thin clients, using an FTP server:

- Dell Wyse Z50D
- Dell Wyse D90D7

Procedure

1. Start the Wyse thin client and log on using `admin` as user name and password.
2. Perform the following steps to configure an INI server manually:
   a. Select **Computer** > **Control Center** > **INI and Upgrade Settings**.
   b. Select one of the following options:
      - **Use INI files from server only**
      - **Use local INI files**
   c. Clear the **Get INI and Upgrade server details via DHCP** check box.
   d. In the **INI Server URL** field, enter the URL of the FTP server where the Avaya Agent for Desktop installation file is located.
   e. Select the **Server requires authentication** check box.
   f. Enter the user name and the password of the FTP server.
   g. Click **OK**.
3. Perform the following actions to configure the Image Upgrade options:
   a. Double-click **INI and Upgrade Settings**.
   b. In the **INI and Upgrade Network Settings** dialog box, click **Image Upgrade Settings**.

      The system displays the Thin Client Settings dialog box.
   c. In the **Update Mode** field, select **Add-ons Only**.

d. In the **Update Server URL** field, enter the URL of the FTP server where Avaya Agent for Desktop is located.
e. Select the **Server requires authentication** check box.
f. Enter the user name and the password of the FTP server.
g. Select the **Restore factory defaults when updating** check box.
h. Click **OK**.

4. Restart the Wyse thin client.

Related links

Installation checklist on page 29

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 t610 or HP t510 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.

Related links

Installation checklist on page 29

Uninstalling Avaya Agent for Desktop from a Dell Wyse thin client

Before you begin

Stop Avaya Agent for Desktop.

About this task

Procedure

1. Click **Control Center** > **Novell Add-on Manager**.
2. Find the Avaya Agent for Desktop package in the list and clear the corresponding check box.
3. Click **Execute**.
4. Click **Control Center** > **More Applications** and verify that Avaya Agent for Desktop is removed.

Related links

Installation checklist on page 29

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.

Related links

Installation checklist on page 29

Installing Avaya Agent for VDI remotely

Installing Avaya Agent for Desktop using WDM

Before you begin

Before installing Avaya Agent for Desktop, ensure that the FTP Server is installed.

About this task

This procedure describes the steps to install Avaya Agent for Desktop on the following Suse Linux-based Dell Wyse thin clients, using the Wyse Device Manager (WDM):

- Wyse Z50D

Procedure

1. Run **Start** > **All Programs** > **Wyse Device Manager** > **Script Builder**.
2. In the Script Builder window, enter the package name, the package category, the package description and the operating system.

   For example:

   - Package name: Install Avaya Agent
   - Package category: Other Packages
   - Package description: Install Avaya Agent
   - Operating system: Suse Linux
3. Use the following script to install Avaya Agent for Desktop:

```
[Version]
Number=InstallAvaya_Agent To_SLETC
Description=Installation Avaya Agent to Wyse SLETC
OS=SLX
Category=Other Packages
USE_REMOTE=Yes
; Date: 3/12/2012

[Script]
SF "<regroot>/avaya-agent-0.0.0.xxxx-1.sletc11sp1.rpm" "/tmp/avaya-
agent-0.0.0.XXXX-1.sletc11sp1.rpm"
EX "rpm -i  -nodeps /tmp/avaya-agent-0.0.0.XXXX-1.sletc11sp1.rpm"</regroot
>
```

   Note:

   You must replace the XXXX sequence with the version number in the downloaded .rpm file.
4. Save the script in a directory.

   For example, you can name the script as `Avaya_Agent-install`.

   WDM creates a directory with the name that you provide for the script.

5. Copy the Avaya Agent for Desktop package, `avaya-agent-0.0.0.XXXX-1.sletc11sp1.rpm`, into the directory with the script name.
6. Start Wyse Device Manager.
7. In the Console Root folder, select **WyseDeviceManager** > **Package Manager** > **Other Packages**.
8. Right-click Other Packages and select **New**.
9. Select **Register a Package from a Script file**.
10. Enter the full path of the script file and click **Next** until the package registration process starts.
11. Click **Finish**.
12. To install Avaya Agent for Desktop on one or more devices, perform the following actions:
    a. In the Console Root folder, select **WyseDeviceManager** > **Device Manager**.
    b. Select one or more devices from the list.
    c. Right-click one of the devices and select **Package Distribution Wizard**.
    d. Select **Other Packages**.
    e. Select the script from the package list and click **Next** until the updates are scheduled.
    f. Click **Finish**.

Related links

Installation checklist on page 29

Uninstalling Avaya Agent for Desktop using WDM

Procedure

1. Run **Start** > **All Programs** > **Wyse Device Manager** > **Script Builder**.
2. In the Script Builder window, enter the package name, the package category, the package description and the operating system.

   For example:

   - Package name: UninstallAvayaAgent_from_SLETC
   - Package category: Other Packages
   - Package description: Install Avaya Agent
   - Operating system: SLX
3. Use the following script to uninstall Avaya Agent for Desktop:

```
[Version]
Number=UninstallAvayaAgent_from_SLETC
Description=Uninstall Avaya Agent from Wyse SLETC
OS=SLX
Category=Other Packages
USE_REMOTE=Yes
; Date: 3/12/2012
```

```
[Script]
EX "rpm -e Avaya-Agent"
```

4. Save the script.
5. Start Wyse Device Manager.
6. In the Console Root folder, select **WyseDeviceManager** > **Package Manager** > **Other Packages**.
7. Right-click Other Packages and select **New**.
8. Select **Register a Package from a Script file**.
9. Enter the full path of the script file and click **Next** until the package registration process starts.
10. Click **Finish**.
11. To remove Avaya Agent for Desktop from one or more devices, perform the following actions:
    a. In the Console Root folder, select **WyseDeviceManager** > **Device Manager**.
    b. Select one or more devices from the list.
    c. Right-click one of the devices and select **Package Distribution Wizard**.
    d. Select **Other Packages**.
    e. Select the script from the package list and click **Next** until the updates are scheduled.
    f. Click **Finish**.

Related links

Installation checklist on page 29

Installing Avaya Agent for Desktop on t610 and 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 t610 and 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.

Related links

Installation checklist on page 29

Installing Avaya Agent for Desktop on t510 and t520 HP ThinPro 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

Use this procedure to install Avaya Agent for Desktop on an HP t510 and t520 ThinPro 5.0 OS-based thin client by using HP Device Manager (HPDM).

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-1.1.0.3003-thinpro50.deb
    rm /tmp/avaya-agent-1.1.0.3003-thinpro50.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.

Related links

Installation checklist on page 29

Uninstalling Avaya Agent for Desktop from t610 and 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.

Related links

Installation checklist on page 29

Uninstalling Avaya Agent for Desktop from t510 and t520 HP ThinPro using HPDM

Procedure

1. Start the HPDM console.
2. On the **HP ThinPro 5** 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.

Related links

Installation checklist on page 29

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 License Agreement screen.
5. Read the agreement carefully and select **I accept the agreement** to accept the terms and conditions.
6. Click **Next** .

The system displays the Destination screen.

7. Specify the installation destination and click **Next** .

   The system displays the Select Start Menu Folder screen.

8. Specify the folder name and click **Next** .

   The system displays the click to dial Browser Extension screen.

9. 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.

10. Select the required options and click **Next**.

    The system displays the Ready to Install screen.

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 End User License Agreement window.

13. Click **Install**.

    The Avaya Agent for Desktop is installed on your system and confirmation screen is displayed.

14. Ensure that the **Launch Avaya Agent** check box is selected and click **Finish**.

    The system displays the Avaya Agent for Desktop Welcome window.

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

16. Click **Next**.

    The system displays the End User License Agreement (EULA) screen in the selected UI langauge.

17. Read the agreement carefully and select **I Agree** to accept the Avaya Agent for Desktop EULA.

18. Click **Next**.

    The system displays the License Type screen.

19. 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.

20. 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 Configuration settings later. Avaya Agent for Desktop would still work in 30 days trial mode with functionality of the chosen license type.

The system displays the Ready screen.

21. Click **Launch**.

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

Related links

Installation checklist on page 29

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.

Related links

Installation checklist on page 29

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, .zip) saved at the download location.

   The system extracts the .zip file and creates a folder which contains Avaya Agent for Desktop application.
3. Open the Avaya Agent for Desktop folder.

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 Configuration settings later. Avaya Agent for Desktop would still work in 30 days trial mode with functionality of the chosen license type.

    The system displays the Browser extension screen.

11. For Google Chrome, do the following:
    a. Select the **Google Chrome** check box.
    b. Open the Google Chrome browser window and navigate to the extensions page.
    c. Open the Avaya Agent for Desktop window and drag **BrowserExtension.crx** and drop it to Google Chrome page.

       The Avaya Agent for Desktop browser extension for Google Chrome is installed.

12. For Mozilla FireFox, do the following:
    a. Select the **Mozilla Firefox** check box.
    b. Click **Install FireFox Extension**.

       The Avaya Agent for Desktop browser extension for Mozilla Firefox is installed.

13. Click **Next**.

    The system displays the Ready screen.

14. Click **Launch**.

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

Related links

Installation checklist on page 29

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

Procedure

1. Open the **Applications** folder.
2. Drag and drop the Avaya Agent for Desktop application icon to **Trash**.

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

Related links

Installation checklist on page 29

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. You also need to install a separate license on WebLM server for a headless mode. This license must support the feature `VALUE_VDIA_HEADLESS_ONLY_COUNTS` for activating a headless mode.

Related links

Installation checklist on page 29

Installing Avaya Agent for Desktop for headless mode

About this task

Ensure that you have downloaded the latest installer specifically created for a headless mode. You must follow the regular installation instructions as per your requirement as mentioned in the other sections of the guide for the various installation platforms.

Related links

Installation checklist on page 29

Checklist for configuring Avaya Agent for Desktop for a headless mode

Configuration window

Note:

Refer to the configuration settings field description 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	Only the Skip Log in Dialog can be configured. Rest all fields are disabled.
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 will be available for a particular license type. Refer the following table for more details:

Table 4:

License types/Features	Advanced/Standalone	Basic / (Shared Controlled with Avaya one-X® Agent)	Locked Down/ Headless
Full UI	Yes	Yes	N/A
Headless UI	N/A	N/A	Yes
Collapsed UI Media Controls	Yes	Yes	N/A
H.323 Roadwarrior	Yes	Yes	Yes
SIP Roadwarrior	Yes	Yes	Yes
Desk Phone Mode	Yes	N/A	N/A
Other Phone/ Telecommuter	Yes	N/A	N/A
Media Quality Indicator	Yes	Yes	N/A
Dual Registration/Failover	Yes	Yes	Yes
Stats Console	Yes	N/A	N/A
Screen Pop	Yes	N/A	N/A
VoIP Quality Monitoring	Yes	Yes	Yes

Table continues…

Supervisor Features	Yes	N/A	N/A
CTI Controlled	Yes	Yes	Yes

Other capabilities

- Log in on the extension using the Login dialog box.
- Use the CTI application or another client to register 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.

Related links

Installation checklist on page 29

Performing silent installation of Avaya Agent for Desktop

Procedure

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

   ```
   /SILENT /LICENSE TERMS ACCEPTANCE = TRUE
   ```

   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:

   ```
   /verysilent /LICENSE TERMS ACCEPTANCE = TRUE
   ```

   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:

   ```
   /verysilent /LICENSE TERMS ACCEPTANCE = TRUE /
   LOG="<InstallationLogPath>"
   ```

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

Assigning functions to buttons in Avaya Aura® Communication Manager

About this task

To assign functions to the Dial Pad buttons in the Avaya Agent for Desktop user interface, perform the following actions:

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 functions to the Dial Pad buttons in the Avaya Agent for Desktop user interface for SIP users in Avaya Aura® System Manager, perform the following actions:

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, and 9611 SIPCC 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`

   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 using the Configuration menu

Familiarizing with the Avaya Agent user interface

Configuration menu

Server tab field descriptions

ACM Login Type:

Important:

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

Name	Description
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.
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.
Use Local Configuration	The field to enable or disable the use of a local configuration. When the **Use Local Configuration** check box is selected, the agent profile uses the configuration defined on the local system. When the **Use Local Configuration** check box is clear, Avaya Control Manager settings are enabled and all the fields in the **Local Server Settings** field are inactive. Supports both H.323 and SIP signalling.

Avaya Control Manager Settings:

The **Avaya Control Manager Settings** field is enabled when the **Use Local Configuration** check box is clear.

Note:

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

Important:

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

Name	Description
Primary Avaya Control Manager 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 Avaya Control Manager 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.
Avaya Control Manager profile type	The field to configure the profile type. The available options are: • **ONEX Agent**: Select this option if you want to use Avaya one-X® Agent profile settings from Avaya Control Manager 7.1.2 or 8.0. • **Avaya Agent**: Select this option if you want to use Avaya Agent for Desktop plug-in for Avaya Control Manager 7.0.

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`

Name	Supported signalling	Description
		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
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 SBC server IP address.
Secondary SIP Proxy address	SIP	The field to configure the IP address of the secondary SIP proxy server.

Table continues…

Name	Supported signalling	Description
		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 SBC HA server IP address.
SIP domain	SIP	The field to configure the domain name for SIP.
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

Table continues…

Name	Supported signalling	Description
		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.
Directory address and port	Both H.323 and SIP	The field to specify the network domain or the IP address and the port of the public directory server.
Directory search root	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.
Directory 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.

Table continues…

Name	Supported signalling	Description
		• **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.

Dialing Rules tab field descriptions

Dialing Rules

Name	Description
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.
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.
Number to dial to access an external line	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 long distance calls	The field to specify the national long distance prefix. For example, in North America, type 1.
Number to dial for international calls	The field to specify the international prefix. For example, in North America, type 011.
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.
User 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

Table continues…

Name	Description
	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.

Preferences tab field descriptions

Main section:

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.
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.
CM Auto Answer Support Required	Select this option if your administrator has configured the extension on Avaya Aura® Communication Manager to support Auto Answer.
Skip Log in dialog	The system does not display the window to log in to the station and registers the agent automatically.
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** feature.

Table continues…

Name	Description
	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** time unlimited.
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**.
Allow Manual Call After Work	Select to change to the After Call Work state manually.
Local Auto Answer	Use this option for Avaya Agent for Desktop to answer the call automatically. Ensure that **Auto answer** is also enabled in Avaya Aura® Communication Manager to make this option work properly.
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.
Enable Drop Call Button	Select this option to enable drop call button on the Avaya Agent for Desktop active call appearance section.

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.

Type of Transfer/Conference:

Name	Description
Transfer type	A drop-down list displaying two options: • **Direct**: To transfer the calls automatically. • **Consultative**: To talk to the client yourself before performing a transfer.
Conference type	A drop-down list displaying two options: • **Direct**: To create the conference automatically.

Table continues…

Name	Description
	• **Consultative**: To talk to the client yourself before creating the conference.

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. • **Other Phone**: Use this option to use the Avaya Agent for Desktop in a Telecommuter mode. You need to define the telecommuter 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.
Telecommuter Number	The field to define the telecommuter or other phone number. For example, an office desk phone number or a mobile phone number.

Startup Message:

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

Reason Codes field descriptions

Avaya Agent for Desktop supports three classes of reason codes: Auxiliary, Call Work, and 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 appear 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 will receive an error when they try to change the Auxiliary reason code manually.

Name	Description
Type	The field for selecting the list of reason codes to display. The reason codes that you can define are of the following types: • **Auxiliary**: The reasons for changing to the AUX state. • **Log Out**: The reasons for logging out from the ACD service. • **Call Work**: The reason for taking any call work related action during an active call.
Reason Code	The digit string that represents the reason code. This string is displayed on the top bar on selection.
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.

Audio tab 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.
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.
Call Button	Defines the call controls options for headset call button. Use the following options: • **Disabled** • **Answer** • **Hold** • **Drop**
Auto Gain Control	Automatically controls the audio volume of a call.
Echo Cancellation	Suppresses any possible echo in a call.
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.

Table continues…

Name	Description
	• **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.

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	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	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.
File name	The field to display the file name of the active audio file.
Duration	This field displays the duration of the recorded audio greeting.

Icon	Name	Description
	**Add**	Add a new greeting to the greetings table.
	**Remove**	Remove a greeting from the greetings table.
	**Move upward**	Move the selected greeting upward in the greetings table.
	**Move downward**	Move the selected greeting downward in the greetings table.
	**Settings**	Click to record or upload a an audio files. The settings button appears when the cursor is hovered over an entry in the greeting list. Audio settings dialog box field descriptions. • **Add (****)**: Adds a new audio greeting message. • **Remove (****)**: Removes already saved audio greeting message • **Browse**: Browses to select an audio greeting message in your repository. • **Record (****)**: Records a new audio greeting message. • **Name**: Displays the name of the selected audio greeting message. • **Play (****)**: Plays a recorded audio greeting message. • **Path**: Displays the location where the recorded audio greeting message is saved. • **Duration**: Displays the duration of the audio greeting message.
	**Play**	Plays an existing greeting message. The play button appears when the cursor is hovered over an entry in the greeting list.

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.
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`.
Params	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 that Communication Manager collected from a centralized application. Although UUI supports 96 bytes of information, Avaya Agent for Desktop supports only the first 32 bytes of information. • <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.

Table continues…

Name	Description
	• <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.
Type	The field to specify whether you want to open an application or a web URL in an external or an internal browser.
Trigger when an incoming call is	The field to indicate when the program must trigger the Screen Pop for an incoming call: • **Ringing**: To open Screen Pop when the phone rings. • **Answered**: To open Screen Pop when an agent answers the call using the Avaya Agent for Desktop GUI. • **Missed**: To open Screen Pop when the call appearance from an incoming call disappears after no response and the caller hangs up. • **Released**: To open Screen Pop when an incoming call is dropped or disconnected by an agent or a customer.
Trigger when an outgoing call is	The option to indicate when the program must trigger the Screen Pop for an outgoing call: • **Connected**: To open Screen Pop when the called-party answers the phone. • **Released**: To open Screen Pop when an outgoing call is dropped or disconnected by an agent or a customer.
Trigger only when the VDN is	The option to open Screen Pop for a specific VDN added in the corresponding field. **Note:** For Screen Pop to run, you must enter the VDN name (up to 15 characters) in the field.
Use internal browser for ACM and Breeze screen pops by default	The option to open ACM or Breeze web URL screen pops in an internal browser.

Icon	Name	Description
	Add	To add a new entry in the Screen Pop list.
	Remove	To remove an entry from the Screen Pop list.

Security tab field descriptions

Password Storage

Name	Description
Allow to use non-secure storage if security storage is unavailable	The option to allow a password to load from non-secure storage if security storage is not available.

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.
Use local	The option to select the third-party certificate installed on 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.
Use remote host	The option to select the third-party certificate located on a remote server. You can choose to select the certificate from an http or an https location. You must provide the IP address and the 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.

Table continues…

Name	Description
	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. Also, you must compulsorily download the **cert.pem** file from the remote server to the **certs** folder of Avaya Agent for Desktop.

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.

Advanced tab field descriptions

Language section

Name	Description
Language	The language of the Avaya Agent for Desktop user interface. The supported UI languages are: • 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

Logs 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: • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **Info** • **Debug**

Table continues…

Name	Description
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. • **Emergency** • **Alert** • **Critical** • **Error** • **Warning** • **Notice** • **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.
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 quality logs	When the **Include media quality logs** check box is selected, media quality logs are included in the remote logs.

Table continues…

Name	Description
	Note: You must select the **Include media quality logs** check box to view **RTCP Monitoring Server Settings** section in the **Advanced** tab.

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.

QoS 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.
Audio DSCP	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.

Presence

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

Configuring the connection to Avaya Control Manager

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Configuration**. The system displays the Avaya Agent for Desktop Configuration 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 Configuration window, click the **Server** tab.
2. In the ACM Login Type section, 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 **Avaya Control Manager Settings** field, 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. To download the protocol specific ONEXAgent profile from ACM, select **Use Local Configurations**.

7. Select the required **Signalling** option.
8. Clear the **Use Local Configuration** check box.
9. Click **Save**.
10. Restart the Avaya Agent for Desktop application.

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 **Configuration**. The system displays the Avaya Agent for Desktop Configuration 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 Configuration window, click the **Server** tab.
2. In **ACM Login Type**, select **Use Local Configurations**.
3. 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.

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 **Configuration**. The system displays the Avaya Agent for Desktop Configuration 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 Configuration window, select the **Server** tab.
2. In **ACM 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.

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 **Configuration**. The system displays the Avaya Agent for Desktop Configuration 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 Configuration window, click the **Server** tab. remove from Before you begin and make that Step 1.
2. In **ACM 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 SBC server 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. **(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 SBC HA server IP address.

7. **(Optional)** In the corresponding fields, specify the port number and the port type.
8. 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.
9. Click **Save**.
10. Restart the Avaya Agent for Desktop application.

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 agent 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.

Related links

Configuring Avaya Agent for Desktop for using SIP shared control mode on page 76

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 **Configuration**. The system displays the Avaya Agent for Desktop Configuration 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 TCP and set 5060 as the port number.

Procedure

1. In the Avaya Agent for Desktop Configuration window, click the **Server** tab.
2. In **ACM 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 SBC server 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 75

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 **Configuration**. The system displays the Avaya Agent for Desktop Configuration 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. In the Avaya Agent for Desktop Configuration window, select the **Server** tab.
2. Click one the following options:
   - **H.323**
   - **SIP**
3. In the **Directory address and port** field, enter the URL of the network domain or the IP address and the port of the public directory server.
4. In the **Directory search root** field, enter an LDAP format string representing an information type.

   To configure the **Directory search root** 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.
5. 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.
6. 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.
7. 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.

8. Click **Save**.

   Note:

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

9. Restart the Avaya Agent for Desktop application.

Configuring the dialing rules

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Configuration**. The system displays the Avaya Agent for Desktop Configuration 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 Configuration window, select the **Dialing Rules** tab.
2. In the **Dialing Rules** section, do the following:
   a. In the **Internal extension length** field, specify the length of the internal extension calls.
   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.
   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**.

Enabling the auto answer feature

Before you begin

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

About this task

Enable the auto answer feature for the system to answer the calls automatically.

Procedure

1. Click the **Preferences** tab.
2. In the **Main** field, perform one of the following actions:
   - select the **Local Auto Answer** check box to enable local auto answer.
   - clear the **Local Auto Answer** check box to disable local auto answer.

   Note:

   It is essential that the **CM Auto Answer Support Required** check box be synchronized with the Auto Answer setting of Avaya Aura® Communication Manager. If these two options are not synchronized, Avaya Agent for Desktop does not function properly.

   If the CM **Auto Answer** option is set to none, the **CM Auto Answer Support Required** check box must be clear. With other CM Auto Answer options, such as *all*, or *acd*, the **CM Auto Answer Support Required** check box must be selected.

   If the CM Auto Answer is set to *all*, the setting on Avaya Aura® Communication Manager takes precedence and Avaya Agent for Desktop answers all the incoming calls automatically, with disregard to the Local Auto Answer setting.

3. Click **Save**.

Enabling the drop call button

Before you begin

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

About this task

Enable the drop call button to drop a call from the call appearance section.

Procedure

1. Click the **Preferences** tab.
2. In the **Main** field, select the **Enable Drop Call Button** check box.
3. Click **Save**.

Configuring the ready mode option

Before you begin

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

Procedure

1. Click the **Preferences** tab.
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**.

Example

Next steps

Configuring the after call work settings

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Configuration**. The system displays the Avaya Agent for Desktop Configuration 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 Configuration window, click the **Preferences** tab.
2. (Optional) In the **Main** 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 **Main** 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 and interface settings

Before you begin

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

Procedure

1. In the Avaya Agent for Desktop Configuration window, click the **Preferences** tab.
2. In the **Main** field, perform the following actions:
   - Select the **Automatically log in agent** check box to log automatically to the user on ACD after the system successfully registers 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.
   - Select the **Skip login dialog** check box to not display the login dialog box and register the agent automatically.
   - Select the **Launch Avaya Agent when Windows starts** check box to open the Avaya Agent for Desktop application at Windows startup.
   - Select the **Show user interface** check box to unhide and display the interface of the Avaya Agent for Desktop application.

- Select the **Always Display The Main Window on Top** check box to keep the main Avaya Agent for Desktop window on top of all your screen windows.

3. Click **Save**.

Configuring the Login mode settings

Before you begin

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

Procedure

1. In the Avaya Agent for Desktop Configuration window, click the **Preferences** tab.
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**.

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. 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:
   a. Coach: listen-only

b. Coach: listen/talk

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.

Related links

Enabling the supervisor feature from an existing database contact on page 83
Enabling the supervisor feature from the main screen input box on page 84

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 supervise 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

Ensure that agent is logged in as a supervisor.

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:
   - Coach: listen-only
   - Coach: listen/talk

   Note:

   - Avaya Agent for Desktop uses the feature button FAC in the background to activate this feature.
   - Avaya Agent for Desktop also suppresses the quick call appearance that pops-up the feature activation.
   - 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.
   - In case of a **Listen-Only** session, the agent receives the session as muted as a standard.
   - The supervisor can stay during the entire call, unmute the call, or hang-up the call.
   - After the call ends, the system goes back to the normal state as a regular station.

Related links

Avaya Agent for Desktop supervisor feature overview on page 82

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

Ensure that agent is logged in as a supervisor.

Procedure

1. Click and select anyone of the following options:
   - Coach: listen-only
   - Coach: listen/talk
2. Type the agent id/VDN in the main screen input box and press Enter.

Note:

- Avaya Agent for Desktop uses the feature button FAC in the background to activate this feature.
- Avaya Agent for Desktop also suppresses the quick call appearance that pops-up the feature activation.
- 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.
- In case of a **Listen-Only** session, the agent receives the session as muted as a standard.
- The supervisor can stay during the entire call, unmute the call, or hang-up the call.
- After the call ends, the system goes back to the normal state as a regular station.

Related links

Avaya Agent for Desktop supervisor feature overview on page 82

Configuring the transfer and the conference types

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Configuration**. The system displays the Avaya Agent for Desktop Configuration 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 Configuration window, click the **Preferences** tab.
2. In the **Type of Transfer/Conference** field, select the type of transfer and the type of conference.
3. Click **Save**.

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 Configuration window

Related links

Adding a user in Avaya Aura Messaging on page 85
Configuring the message waiting indicator settings on page 86

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**.

Related links

Message waiting indicator overview on page 85

Configuring the message waiting indicator settings

Before you begin

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

   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**.

Related links

Message waiting indicator overview on page 85

Configuring the startup message

Before you begin

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

Procedure

1. In the Avaya Agent for Desktop Configuration window, click the **Preferences** tab.
2. In the **Startup Message** field, enter the disclaimer message to display when Avaya Agent for Desktop starts.

3. Click **Save**.

Adding reason codes

Before you begin

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

About this task

Avaya Agent for Desktop supports three classes of reason codes: Auxiliary, Call Work, and 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 appear 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 (✔).

Procedure

1. In the Avaya Agent for Desktop Configuration window, click the **Reason Codes** tab.
2. In the **Type** field, select the reason code type to display:
   - **Auxiliary**: The reasons for changing to the AUX state.
   - **Log Out**: The reasons for logging out from the ACD service.
   - **Call Work**: The reason for taking any call work related action during an active call.
3. Click the **+** button.
4. In the **Reason Code** field, double-click the number and type the number to associate to the reason code.
5. In the **Description** field, type the description of the reason code.
6. Click **Save**.

Removing reason codes

Before you begin

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

About this task

Avaya Agent for Desktop supports three classes of reason codes: Auxiliary, Call Work, and 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 appear 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 (✔).

Procedure

1. In the Avaya Agent for Desktop Configuration window, click the **Reason Codes** tab.
2. In the **Type** field, select the reason code type to display:
   - **Auxiliary**: The reasons for changing to the AUX state.
   - **Log Out**: The reasons for logging out from the ACD service.
   - **Call Work**: The reason for taking any call work related action during an active call.
3. Click the reason code that you must remove.
4. Click the **–** button.
5. Click **Save**.

Configuring the audio input

Before you begin

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

Procedure

1. In the Avaya Agent for Desktop Configuration window, click the **Audio** tab.
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 **Configuration**. The system displays the Avaya Agent for Desktop Configuration window.

Procedure

1. In the Avaya Agent for Desktop Configuration window, select the **Audio** tab.
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 **Configuration**. The system displays the Avaya Agent for Desktop Configuration 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 DesktopConfiguration window, select the **Audio** tab.
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 **Configuration**. The system displays the Avaya Agent for Desktop Configuration 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 DesktopConfiguration window, select the **Audio** tab.
2. In the **Audio Advanced Settings** area, from the **Control Device** drop-down list, select the available headset option.
3. 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**

4. Select the **Auto Gain Control** check box to automatically control the audio volume of a call.
5. Select the **Echo Cancellation** check box to suppress any possible echo in a call.
6. In the **Noise Suppression** field, click one of the following options to suppress noise in a call:
   - **Disabled**
   - **Conference**
   - **Low**
   - **Moderate**
   - **High**
   - **Very High**
7. Click **Save**.

Adding a greeting message

Before you begin

In the system tray, right-click the Avaya Agent for Desktop icon and select **Configuration**. The system displays the Avaya Agent for Desktop Configuration 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 Configuration window, select the **Greetings** tab.
2. Click the **Add** icon.
3. Double-click the **Rule Name** field and type the name of the greeting message.
4. Double-click the **VDN Name** 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** 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. In the **Duration** field, click the **Settings** icon to start recording or uploading a greeting message.
7. In the **Greeting** dialog box, click **Add** to add a new audio message.
8. To record an audio file, select an entry from the **Greetings List** and click the **Record** icon.
9. To rename an audio file, select the file and double-click the file to edit the file name.
10. (Optional) Click the **Play** icon to listen to the recording.

    To upload an audio file for a greeting message, select an entry from the **Greetings List** and click **Browse** and upload a new audio file.
11. To remove an audio file from the **Greetings List** , select an entry from the list and click the **Delete** icon.
12. Click **Yes** to confirm deletion.
13. To activate an audio file for a greeting message, from the **Greetings List** section, select an audio file.
14. Click **Save** to save the audio file configuration.
15. Click **Save** to save the greeting message configuration.

Removing a greeting message

Before you begin

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

Procedure

1. In the Avaya Agent for Desktop Configuration window, click the **Greetings** tab.
2. Select the greeting.
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 **Configuration**. The system displays the Avaya Agent for Desktop Configuration window.

Procedure

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

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 Configuration window, click the **Screen Pop** tab.

   The system displays the Screen Pop screen.

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

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

3. In the **Name** list, click and rename the untitled field.
4. 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.

5. In the **Params** field, type the required parameter. .
6. In the **Type** field, click one of the following :
   - **Application**: To browse and specify the path for an application on the local system.
   - **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.
7. To indicate when the application must trigger the Screen Pop for inbound calls, from **Triggers when an incoming call is**, select the appropriate trigger.
8. To indicate when the application must trigger the Screen Pop for outbound calls, from **Triggers when an outgoing call is**, select the appropriate trigger.
9. To open a Screen Pop application for a specific VDN, select **Trigger only when VDN is** and type the VDN name in the corresponding field.
10. To use internal browser for ACM and Breeze, select the **Use internal browser for ACM and Breeze screen pops by default** check box.
11. Click **Save**.

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 **Configuration**. The system displays the Avaya Agent for Desktop Configuration 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, select the **Advanced** tab.
2. In the **Language** field, select 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 **Configuration**. The system displays the Avaya Agent for Desktop Configuration 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 Configuration window, select the **Advanced** tab.
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:
   - **Emergency**
   - **Alert**
   - **Critical**
   - **Error**
   - **Warning**
   - **Notice**
   - **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 **Configuration**. The system displays the Avaya Agent for Desktop Configuration 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 Configuration window, select the **Advanced** tab.
2. In the **RTCP Monitoring Server Settings** section, perform the following actions:
   a. In the **Address** field, type the IP address of the RTCP server.
   b. In the **Port** field, type the port number of the RTCP server.
   c. In the **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 **Configuration**. The system displays the Avaya Agent for Desktop Configuration 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 Configuration window, select the **Advanced** tab.
2. In the **QoS tagging for audio** 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.
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 **Configuration**. The system displays the Avaya Agent for Desktop Configuration 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 Configuration window, select the **Advanced** tab.
2. In the **QoS tagging for audio** 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 **Signalling DSCP** check box and type the required Signalling DSCP value.

      For more information on DSCP values, see `Commonly used signalling DSCP values`.
   c. Select the **Signalling 802.1 p** check box and type the required Signalling 802.1 p value.
3. Click **Save**.

Configuring the password storage settings

Procedure

1. In the Avaya Agent for Desktop Configuration window, click the **Security** tab.
2. In the **Password Storage** section, select the **Allow to use non-secure storage if security storage is unavailable** check box.
3. Click **Save**.
4. Restart the Avaya Agent for Desktop application.

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.

Configuring the PPM Secure Mode settings

Before you begin

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

About this task

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

Procedure

1. In the Avaya Agent for Desktop Configuration window, click the **Security** tab.
2. In the **PPM Secure Mode** section, click one of the following options:
   - **HTTP**
   - **HTTPS**
3. Click **Save**.

Configuring the 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 Configuration window, click the **Security** tab.
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.
   - **Use remote host**: Click this option to select the third-party certificate from the remote server. You must provide the required IP address and port number of the remote server.
3. Click **Save**.
4. Restart the Avaya Agent for Desktop application.

Configuring the SRTP settings

Procedure

1. In the Avaya Agent for Desktop Configuration window, click the **Security** tab.
2. In the **SRTP** section, select the **Enable SRTP** check box to activate SRTP settings.

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

   Note:

   You must configure the Avaya Communication Manager SRTP 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 Configuration 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 5:

Main window icon	Agent State tooltip	Presence	Presence Note

Table continues…

	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	-

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 6:

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.

Related links

Activating the Presence feature settings on page 100

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 configuration settings and configure SIP endpoint for Presence Services

Procedure

1. In the Avaya Agent for Desktop Configuration window, click the **Advanced** tab.
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.

Related links

Avaya Agent for Desktop Presence feature overview on page 98

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

Table continues…

DSCP value	Hex value	Decimal value	Meaning	Drop probability	Equivalent IP precedence value
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

Lock Manager overview

Avaya Agent for Desktop now provides option to lock a configuration tab or a section in a configuration tab from modification. For preventing the configuration 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 `Lock Manager.xml`.

Sample Lock Manager XML file

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

Related links

Lock Manager lock name for UI controls on page 102

Lock Manager lock name for UI controls

Normal Mode UI Controls

Login dialog

UI control placement	UI control name
Station extension	LoginDialog_StationLoginLineEdit
Station password	LoginDialog_StationPasswordLineEdit
Agent extension	LoginDialog_AgentLoginLineEdit
Agent password	LoginDialog_AgentPasswordLineEdit
Automatically log in	LoginDialog_AgentAutoLoginCheckBox
Login mode	LoginDialog_LoginModeComboBox
TC number	LoginDialog_TelecommuteNumberEdit
Configuration button	LoginDialog_ConfigBtn
Login button	LoginDialog_LoginBtn
Exit button	LoginDialog_CancelBtn

Main window

UI control placement	UI control name
Contacts button	MainWindow_BtnContacts
History button	MainWindow_BtnHistory

Main window drop down menu

UI control placement	UI control name
Agent Register	MainWindow_ActAgentRegister

Contact List

UI control placement	UI control name
Contacts button	MainWindow_BtnContacts
History button	MainWindow_BtnHistory

Contact List

UI control placement	UI control name
History button	MainWindow_BtnHistory
Edit Contact Dialog (Double-click on a contact and click Menu > Edit)	ContactListDialog_EditContactDialog

Table continues…

UI control placement	UI control name
Context menu	ContactListDialog_ContextMenu
Add contact button	ContactListDialog_BtnAddContact
Delete a contact button and Delete an item in a context menu	ContactListDialog_BtnDeleteContact
All contacts button	ContactListDialog_BtAll
Favorites button	ContactListDialog_BtnFavorites
Speed Dial button	ContactListDialog_BtnSpeedDial
Search text box	ContactListDialog_SearchTextBox

History

UI control placement	UI control name
Contacts button	MainWindow_BtnContacts
Context menu	ContactListDialog_ContextMenu
Empty button	ContactListDialog_BtnEmpty
Period button	ContactListDialog_BtnPeriod
Search text box	ContactListDialog_SearchTextBox

Feature Buttons

UI control placement	UI control name
FeatureButton_%displayed_button_name%	displayed_button_name is a button name received from the server. The button name depends on the signaling method in use. For example: FeatureButton_AuxWork for H323; FeatureButton_aux-work for SIP.

Server Tab

UI control placement	UI control name
All controls on the Server tab	ConfigurationDialog_ServerTab
Local Server Settings > Signaling > SIP	ConfigurationDialog_ServerTab_SIPRadioBtn
Local Server Settings > Signaling > H.323	ConfigurationDialog_ServerTab_H323RadioBtn
Local Server Settings > Primary SIP Proxy address	ConfigurationDialog_ServerTab_PrimaryAddressLineEdit
Local Server Settings > Primary SIP Proxy port	ConfigurationDialog_ServerTab_PrimaryAddressPortLineEdit
Local Server Settings > Primary SIP Proxy protocol	ConfigurationDialog_ServerTab_PrimaryAddressProtocolComboBox
Local Server Settings > Secondary SIP Proxy address	ConfigurationDialog_ServerTab_SecondaryAddressLineEdit

Table continues…

UI control placement	UI control name
Local Server Settings > Secondary SIP Proxy port	ConfigurationDialog_ServerTab_SecondaryAddressPortLineEdit
Local Server Settings > Secondary SIP Proxy protocol	ConfigurationDialog_ServerTab_SecondaryAddressProtocolComboBox
Local Server Settings > SIP domain	ConfigurationDialog_ServerTab_DomainLineEdit
Local Server Settings > Number of connection attempts	ConfigurationDialog_ServerTab_MaxAttemptsLineEdit
Local Server Settings > Directory address and port (address)	ConfigurationDialog_ServerTab_DirectoryAddressLineEdit
Local Server Settings > Directory address and port (port)	ConfigurationDialog_ServerTab_DirectoryPortLineEdit
Local Server Settings > Directory search root	ConfigurationDialog_ServerTab_DirectoryRootLineEdit
Local Server Settings > Directory username	ConfigurationDialog_ServerTab_DirectoryUserLineEdit
Local Server Settings > Directory password	ConfigurationDialog_ServerTab_DirectoryPasswordLineEdit
Local Server Settings > Directory bind option	ConfigurationDialog_ServerTab_BindOptionComboBox
Avaya Control Manager Settings > Primary Avaya Control Manager URL	ConfigurationDialog_ServerTab_PrimaryACCCMAddressLineEdit
Avaya Control Manager Settings > Secondary Avaya Control Manager URL	ConfigurationDialog_ServerTab_SecondaryACCCMAddressLineEdit
Use Local Configurations	ConfigurationDialog_ServerTab_UseLocalConfigCheckBox
License Server Settings > License server URL	ConfigurationDialog_ServerTab_LicenseServerUrlLineEdit
Avaya Control Manager Settings > Avaya Control Manager profile type	ConfigurationDialog_ServerTab_TypeOfACMComboBox

Dialing Rules Tab

UI control placement	UI control name
All controls on the Dialing Rules tab	ConfigurationDialog_DialingRulesTab
Internal extension length	ConfigurationDialog_DialingRulesTab_InternalExtentionLengthTextEdit
Local calling area codes	ConfigurationDialog_DialingRulesTab_LocalAreaNumberTextLengthEdit
Length of national phone numbers	ConfigurationDialog_DialingRulesTab_NationalNumberLengthTextEdit

Table continues…

UI control placement	UI control name
Number to dial to access external line	ConfigurationDialog_DialingRulesTab_PrefixDigitsToAccessExternalLineTextEdit
Number to dial for long distance calls	ConfigurationDialog_DialingRulesTab_PrefixDigitsToLongDistanceCallsTextEdit
Number to dial for international calls	ConfigurationDialog_DialingRulesTab_PrefixDigitsToInternationalTextEdit
Your country code	ConfigurationDialog_DialingRulesTab_YourCountryCodeTextEdit

Preferences Tab

UI control placement	UI control name
All controls on the Preferences Tab	ConfigurationDialog_PreferencesTab
Main > Ready Mode > Auto in	ConfigurationDialog_PreferencesTab_ReadyModeAutoInRadioBtn
Main > Ready Mode > Manual in	ConfigurationDialog_PreferencesTab_ReadyModeManualInRadioBtn
Main > Local Auto Answer	ConfigurationDialog_PreferencesTab_AutoAnswerCheckBox
Main > Automatically log in the agent	ConfigurationDialog_PreferencesTab_AutomaticLogInCheckBox
Main > Skip Log in dialog	ConfigurationDialog_PreferencesTab_SkipLoginCheckBox
Main > Timed After Call Work check box	ConfigurationDialog_PreferencesTab_TimedAcwCheckBox
Main > Timed After Call Work Interval Line Edit	ConfigurationDialog_PreferencesTab_TimedAcwInterval
Main -> Timed After Call Work "seconds" label	ConfigurationDialog_PreferencesTab_TimedAcwIntervalLabel
Main -> Allow Manual After Call Work	ConfigurationDialog_PreferencesTab_AllowManualAcwCheckBox
Main > Show user interface	ConfigurationDialog_PreferencesTab_ShowUICheckBox
Type of Transfer/Conference > Transfer type	ConfigurationDialog_PreferencesTab_TransferTypeComboBox
Type of Transfer/Conference > Conference type	ConfigurationDialog_PreferencesTab_ConferenceTypeComboBox
DTMF type > DTMF type	ConfigurationDialog_PreferencesTab_DTMFTypeComboBox
Message Waiting Indicator > Show Message Waiting Indicator	ConfigurationDialog_PreferencesTab_EnableVoiceMessageLine

Table continues…

UI control placement	UI control name
Message Waiting Indicator > Voice Mailbox Number	ConfigurationDialog_PreferencesTab_VoiceNumberLine
Main > CM Auto Answer Support Required	ConfigurationDialog_PreferencesTab_CMAutoAnswerCheckBox
Main > Launch Avaya Agent when Windows starts	ConfigurationDialog_PreferencesTab_AutoStartCheckBox
Main > Always Display The Main Window On Top	ConfigurationDialog_PreferencesTab_AlwaysOnTopCheckBox
All controls on Message Waiting Indicator type group box	ConfigurationDialog_PreferencesTab_MWIGroupBox
All controls on DTMF type group box	ConfigurationDialog_PreferencesTab_typeOfDTMFGroupBox
All controls on Type of Transfer/Conference group box	ConfigurationDialog_PreferencesTab_typeOfTransferConferenceGroupBox
All controls on Login Mode group box	ConfigurationDialog_PreferencesTab_loginModeGroupBox
All controls on Startup Message group box	ConfigurationDialog_PreferencesTab_StartupMessageGroupBox
Login Mode > Login Mode	ConfigurationDialog_PreferencesTab_LoginModeComboBox
Login Mode > Telecommuter Number	ConfigurationDialog_PreferencesTab_TelecommuteNumberLine

Reason Codes Tab

UI control placement	UI control name
All controls on the Reason Codes tab	ConfigurationDialog_ReasonCodesTab
Reason Codes table control	ConfigurationDialog_ReasonCodesTab_TableView
Add Reason Code button control	ConfigurationDialog_ReasonCodesTab_AddItemBtn
Remove Reason Code button control	ConfigurationDialog_ReasonCodesTab_RemoveBtn

Audio Tab

UI control placement	UI control name
All controls on the Audio tab	ConfigurationDialog_AudioTab
Audio Output > Device	ConfigurationDialog_AudioTab_AudioOutputDeviceComboBox
Audio Output > Volume slider control	ConfigurationDialog_AudioTab_AudioOutputVolumeSlider
Audio Output > Test button control	ConfigurationDialog_AudioTab_AudioOutputTestButton

Table continues…

UI control placement	UI control name
Audio Output > Volume Indicator control	ConfigurationDialog_AudioTab_AudioOutputVolumeIndicator
Ringer Output > Device	ConfigurationDialog_AudioTab_RingerOutputDeviceComboBox
Ringer Output > Volume slider control	ConfigurationDialog_AudioTab_RingerOutputVolumeSlider
Ringer Output > Test button control	ConfigurationDialog_AudioTab_RingerOutputTestButton
Ringer Output > Volume Indicator control	ConfigurationDialog_AudioTab_RingerOutputVolumeIndicator
Audio Input > Device	ConfigurationDialog_AudioTab_AudioInputDeviceComboBox
Audio Input > Volume slider control	ConfigurationDialog_AudioTab_AudioInputVolumeSlider
Audio Input > Test button control	ConfigurationDialog_AudioTab_AudioInputTestButton
Audio Input > Volume Indicator control	ConfigurationDialog_AudioTab_AudioInputVolumeIndicator
All controls on Audio Output group box	ConfigurationDialog_AudioTab_audioOutputGroupBox
All controls on Ringer Output group box	ConfigurationDialog_AudioTab_ringerOutputGroupBox
All controls on Audio Input group box	ConfigurationDialog_AudioTab_audioInputGroupBox
All controls on Audio Advanced Settings group box	ConfigurationDialog_AudioTab_audioAdvancedGroupBox

Greetings Tab

UI control placement	UI control name
All controls on the Greetings tab	ConfigurationDialog_GreetingsTab
Configure the VDN greeting messages table control	ConfigurationDialog_GreetingsTab_TableView
Add button control	ConfigurationDialog_GreetingsTab_AddBtn
Remove button control	ConfigurationDialog_GreetingsTab_RemoveBtn
Up button control	ConfigurationDialog_GreetingsTab_UpBtn
Down button control	ConfigurationDialog_GreetingsTab_DownBtn
Table control > Auto Play column	ConfigurationDialog_GreetingsTab_TableView_GreetingAutoplay
Table control > Rule Name and VDN column	ConfigurationDialog_GreetingsTab_TableView_NameAndVdn

Record Dialog

UI control placement	UI control name
Greeting List	RecordDialog_GreetingList
Greeting Name	RecordDialog_LineEditGreeting
Greeting Path	RecordDialog_TextEditPath
Add button	RecordDialog_AddButton
Remove button	RecordDialog_RemoveButton
Browse button	RecordDialog_BrowseBtn

Screen Pop Tab

UI control placement	UI control name
All controls on Screen Pop Tab	ConfigurationDialog_ScreenPopTab

Advanced tab

UI control placement	UI control name
All controls on the Advanced tab	ConfigurationDialog_AdvancedTab
Logs > Log Level	ConfigurationDialog_AdvancedTab_LogLevelComboBox
Logs > Enable Remote Debugging	ConfigurationDialog_AdvancedTab_EnableRemoteLoggingCheckBox
Logs > Include media quality logs	ConfigurationDialog_AdvancedTab_EnableMediaQualityLoggingCheckBox
Logs > Remote Logging Server	ConfigurationDialog_AdvancedTab_RemoteLoggingServerLineEdit
Logs > Remote Log Level	ConfigurationDialog_AdvancedTab_RemoteLogLevelComboBox
Language > Language	ConfigurationDialog_AdvancedTab_LocaleComboBox
QoS tagging > Use local QoS settings	ConfigurationDialog_AdvancedTab_LocalQoSSettingsCheckBox
QoS tagging > Audio DSCP check box control	ConfigurationDialog_AdvancedTab_DSCPCheckBox
QoS tagging > Audio DSCP line edit control	ConfigurationDialog_AdvancedTab_DSCPLineEdit
QoS tagging -> Signaling DSCP check box control	ConfigurationDialog_AdvancedTab_DSCPSigCheckBox
QoS tagging -> Signaling DSCP line edit control	ConfigurationDialog_AdvancedTab_DSCPSigLineEdit
QoS tagging -> Audio 802.1p check box control	ConfigurationDialog_AdvancedTab_Priority802_1CheckBox

Table continues…

UI control placement	UI control name
QoS tagging -> Audio 802.1p line edit control	ConfigurationDialog_AdvancedTab_Priority802_1LineEdit
QoS tagging -> Signaling 802.1p check box control	ConfigurationDialog_AdvancedTab_Priority802_1SigCheckBox
QoS tagging -> Signaling 802.1p line edit control	ConfigurationDialog_AdvancedTab_Priority802_1SigLineEdit
All controls on Language group box	ConfigurationDialog_AdvancedTab_languageGroupBox
All controls on Logs group box	ConfigurationDialog_AdvancedTab_loggingGroupBox
All controls on QoS tagging group box	ConfigurationDialog_AdvancedTab_QoSGroupBox
All controls on RTCP Monitoring Server settings group box	ConfigurationDialog_AdvancedTab_PrognosisServerSettingsGroupBox
All controls on PPM Secure Mode group box	ConfigurationDialog_AdvancedTab_PPMGroupBox
All controls on Third-party certification group box	ConfigurationDialog_AdvancedTab_ThirdPartyCertsGroupBox
All controls on SRTP group box	ConfigurationDialog_AdvancedTab_SRTPGroupBox

Headless Mode UI Controls

The default lock configuration of Avaya Agent for Desktop in a Headless Mode reads from another built-in XML. The following rules are applied to lock controls in a headless mode:

UI control placement	UI control name
All controls on the Dialing Rules tab	ConfigurationDialog_DialingRulesTab
All controls on Reason Codes Tab	ConfigurationDialog_ReasonCodesTab
All controls on Greetings Tab	ConfigurationDialog_GreetingsTab
All controls on Screen Pop Tab	ConfigurationDialog_ScreenPopTab
Preferences Tab > Main > CM Auto Answer Support Required	ConfigurationDialog_PreferencesTab_CMAutoAnswerCheckBox
Preferences Tab > Main > Timed After Call Work check box	ConfigurationDialog_PreferencesTab_TimedAcwCheckBox
Preferences Tab > Main > Timed After Call Work Interval Line Edit	ConfigurationDialog_PreferencesTab_TimedAcwInterval
Preferences Tab > Main > Timed After Call Work "seconds" label	ConfigurationDialog_PreferencesTab_TimedAcwIntervalLabel
Preferences Tab > Main > Ready Mode > Auto in	ConfigurationDialog_PreferencesTab_ReadyModeAutoInRadioBtn
Preferences Tab > Main > Ready Mode > Manual in	ConfigurationDialog_PreferencesTab_ReadyModeManualInRadioBtn

Table continues…

UI control placement	UI control name
Preferences Tab > Main > Launch Avaya Agent when Windows starts	ConfigurationDialog_PreferencesTab_AutoStartCheckBox
Preferences Tab > Main > Always Display The Main Window On Top	ConfigurationDialog_PreferencesTab_AlwaysOnTopCheckBox
Preferences Tab > Main > Local Auto Answer	ConfigurationDialog_PreferencesTab_AutoAnswerCheckBox
Preferences Tab > Main > Show user interface	ConfigurationDialog_PreferencesTab_ShowUICheckBox
Preferences Tab > Main > Automatically log in the agent	ConfigurationDialog_PreferencesTab_AutomaticLoginCheckBox
Preferences Tab > All controls in Message Waiting Indicator type group box	ConfigurationDialog_PreferencesTab_MWIGroupBox
Preferences Tab > All controls in DTMF type group box	ConfigurationDialog_PreferencesTab_typeOfDTMFGroupBox
Preferences Tab > All controls in Type of Transfer/Conference group box	ConfigurationDialog_PreferencesTab_typeOfTransferConferenceGroupBox
Preferences Tab > Login Mode > Login Mode	ConfigurationDialog_PreferencesTab_LoginModeGroupBox
Preferences Tab > Login Mode > Telecommuter Number	ConfigurationDialog_PreferencesTab_StartupMessageGroupBox

Related links

Lock Manager overview on page 101

Breeze integration and feature support

The Invite SIP message with Avaya Breeze integration contains AvayaBreeze-Feature headers which contains information about the breeze features.

The format of the SIP header received from the Avaya Breeze snap-in is as shown in the following table:

```
AvayaBreeze-Feature:
namespace=<TEXT>;featureID=<text>;displayFormat=<NONE | LABEL |
ACTION>;caption=<TEXT>;invokeURI=<APP://URI | HTTP://URI |
HTTPS://URI>;appParams=<TEXT>;os=<WIN | MAC | LINUX |
ALL>;screenPop=<TRUE | FALSE>;autoInvoke=<TRUE | FALSE>
```

The following are the features supported for Avaya Breeze and works only in a TLS connection:

- Avaya Agent for Desktop sends silently the HTTP request if a trigger fires for Avaya Breeze feature.

- Avaya Agent for Desktop displays a screen pop, either in an external or an internal browser, if the trigger fires for Avaya Breeze feature.
- Avaya Agent for Desktop displays the Avaya Breeze feature in a call appearance if the feature is configured as an 'action' and the user of Avaya Agent for Desktop clicks the feature for use.
- Avaya Agent for Desktop updates the label for call appearance if the feature is configured as 'label'.

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

add
greeting message 90
adding a user 85
Avaya Agent
uninstall standalone windows 44
Avaya Agent for Desktop
standalone Mac 44
standalone windows 42
uninstall standalone Mac 46

B

Breeze integration feature support 110

C

checklist
installation 29
Config.xml 96
configuration
audio tab field descriptions 60
reason codes 59
server tab field descriptions 51
configure
add reason codes 87
advanced settings 68
after call work 81
audio, advance 89
audio input 88
audio output 88
auto answer 79
conference type 84
configure ppm secure mode 97
dialing rules 56, 78
drop call button 80
greetings tab field 62
language 93
login and interface settings 81, 82
log level 94
preferences 57
QoS tag, audio 95
QoS tag, signals 96
ready mode 80
remove reason codes 87
ringer output 89
RTCP server 95
security settings 66
startup message 86
transfer type 84
WebLM license URL for H.323 and SIP 72
configure Communication Manager
button assignments 49
configure Communication Manager *(continued)*
configure FTP for Linux 31
configure FTP for Windows 32
configure password storage settings 96
configure security settings 97
configure SRTP settings 97, 100
configure system manager
button assignments 50
connection to Avaya Control Manager 71
connection to Communication Manager 73
connection to SIP proxy server 74

D

deployment process 28
download Avaya Agent 29
downloading software 30

E

enable supervisor feature for an existing contact 83
enable supervisor feature from the main screen input box 84

G

greeting message 90
greeting message order 91

H

hardware requirements
headsets 24
Headless mode configuration checklist 46
headless mode installation 46
headless mode overview 46

I

install
on HP thin client using FTP 34
on Linux using WDM 36
on t510 and t520 HP ThinPro using HPDM 40
on t610 and t620 WES OS using HPDM 38
on Wyse thin clients using FTP 33
Interoperability 26

L

lock manager 101

M

message waiting indicator configuration 86
message waiting indicator overview 85

N

new features 14

O

overview 8

P

PLDS
    downloading software 30
presence overview 98
public directory settings 77

R

related documentation 6
remove greeting message 91
Requirements
    port requirements 22

S

settings
    creating a screen pop 92
    screen pop field descriptions 64
Signalling DSCP values 100
silent installation
    Avaya agent for Desktop 48
SIP shared control mode configuration 76
software requirements
    weblm requirements 23
supervisor feature overview 82
system requirements
    hardware 19
    network 21
    software 19

T

topology 16

U

UI controls lock name 102
uninstall
    from HP client 35
    from t510 and t520 HP ThinPro using HPDM 42
    from t610 and t620 HP WES using HPDM 41
uninstall *(continued)*
    from Wyse client 35
    using WDM 37

V

voice quality of service 21