



Deploying Avaya Contact Center Select Software Appliance

Release 7.1
Issue 03.08
April 2022

© 2015-2022, 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](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](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 type(s)

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time as indicated in the order, Documentation, or as authorized by Avaya in writing. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Heritage Nortel Software

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

Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Avaya, the Avaya logo, Avaya one-X[®] Portal, Avaya Aura[®] Communication Manager, Avaya Experience Portal, Avaya Orchestration Designer, Avaya Aura[®] Session Manager, Avaya Aura[®] System Manager, and Application Enablement Services are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

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

Contents

Chapter 1: Introduction	12
Purpose.....	12
Intended audience.....	12
Related resources.....	12
Avaya Contact Center Select Documentation.....	12
Viewing Avaya Mentor videos.....	14
Support.....	15
Chapter 2: Changes in this release	16
Features.....	16
Ability to deploy Avaya Workspaces at any stage.....	17
Avaya Contact Center Select Release 7.1 Feature Pack 2 Post GA Patches supports Microsoft Windows 11.....	17
Avaya Contact Center Select Release 7.1 Feature Pack 2 Post GA Patches supports Microsoft Windows Server 2019.....	17
Avaya Contact Center Select Release 7.1 supports Microsoft Windows Server 2016.....	18
Avaya Workspaces Service Utility.....	18
Contact Center Manager Administration supported in Microsoft Edge with IE mode.....	18
Ignition Wizard enhancements.....	18
Microsoft Edge support in Agent Desktop.....	18
NTP configuration of the Avaya Workspaces nodes.....	19
Support for Avaya Workspaces.....	19
Support of reverse proxy for Avaya Workspaces.....	19
Other changes.....	19
Avaya Aura [®] Media Server update.....	20
Avaya Aura [®] Media Server update.....	20
Avaya Aura [®] Media Server update.....	20
Documentation update for Avaya Workspaces deployment.....	20
Support for VMware 6.7.....	21
Support for VMware version 7.0.....	21
Support for the latest WebLM release.....	21
Updated third-party software for the Avaya Workspaces cluster.....	21
Updated third-party software for the Avaya Workspaces cluster.....	21
Chapter 3: Overview	22
Chapter 4: Deployment process	25
Chapter 5: Installation checklist	26
Avaya IP Office configuration checklist.....	26
Avaya WebLM deployment checklist.....	27
Avaya Aura [®] Media Server deployment checklist.....	28
Avaya Contact Center Select deployment checklist.....	28

Part 1: IP Office configuration	32
Chapter 6: IP Office configuration	33
IP Office supported versions.....	33
Using IP Office Manager.....	34
Configuring the data synchronization user account.....	35
Configuring an IP Office service user for data synchronization.....	37
Verifying the IP Route configuration.....	38
Configuring the SIP domain name.....	40
Configuring the SIP User Extension number.....	42
Configuring a short code for Contact Center Route Points.....	42
Configuring Contact Recording.....	44
Configuring IP Office extensions.....	48
Saving the IP Office configuration data.....	49
Part 2: Avaya Contact Center Select Software Appliance deployment	51
Chapter 7: Avaya WebLM OVA deployment	52
WebLM OVA.....	52
WebLM OVA deployment procedures.....	53
Deploying the WebLM OVA using vSphere (vSphere desktop client connected directly to ESXi host).....	55
Deploying the WebLM OVA using vCenter (vSphere desktop client connected to vCenter)....	60
Deploying the WebLM OVA using vSphere host client.....	64
Deploying the WebLM OVA using vSphere web client.....	68
Configuring the WebLM virtual machine after deploying using the vSphere Host Client.....	72
Obtaining the WebLM server Host ID.....	73
Installing the WebLM license file.....	75
Chapter 8: Avaya Aura[®] Media Server OVA deployment	77
Avaya Aura [®] Media Server OVA.....	77
Avaya Aura [®] Media Server OVA deployment procedures.....	78
Deploying the Avaya Aura [®] Media Server OVA using vSphere (vSphere desktop client connected directly to ESXi host).....	80
Deploying the Avaya Aura [®] Media Server OVA using vCenter (vSphere desktop client connected to vCenter).....	84
Deploying the Avaya Aura [®] Media Server OVA using vSphere host client.....	89
Deploying the Avaya Aura [®] Media Server OVA using vSphere web client.....	92
Configuring the Avaya Aura [®] Media Server virtual machine after deploying using the vSphere Host Client.....	97
Configuring the Avaya Aura [®] Media Server virtual machine resources.....	98
Logging on to Avaya Aura [®] Media Server Element Manager.....	99
Resetting the Avaya Aura [®] Media Server IP address in Element Manager.....	100
Configuring Avaya Aura [®] Media Server name resolution.....	100
Installing Avaya Aura [®] Media Server updates and patches on a virtual machine.....	101
Chapter 9: Avaya Contact Center Select virtual machine deployment	104

Avaya Contact Center Select virtual machine.....	104
Downloading the most recent documentation.....	106
Creating a VMware virtual machine for Contact Center software.....	106
Installing Microsoft Windows Server 2012 R2.....	113
Contact Center virtual machine hard disks and partitions.....	115
Navigating the Microsoft Windows Server 2012 R2 User Interface.....	116
Installing Microsoft Windows Server 2016 or Windows Server 2019.....	120
Contact Center virtual machine hard disks and partitions.....	122
Navigating the Microsoft Windows Server 2016 or Windows Server 2019 User Interface.....	123
Installing the most recent supported operating system service packs.....	124
Installing VMware Tools.....	125
Connecting to the contact center subnet.....	125
Connecting the server to the network.....	126
Downloading the most recent Contact Center patches to the server.....	126
Enabling Microsoft Remote Desktop connection.....	127
Disabling Admin Approval Mode for Windows Server administrators.....	127
Creating a shared location for security configuration.....	128
Disabling Windows Server Automatic Maintenance.....	129
Installing Avaya Contact Center Select without Avaya Aura® Media Server Release 7.1 DVD software.....	129
Configuring the server installation data.....	133
Enabling Windows Server Automatic Maintenance	144
Using the Contact Center Dashboard.....	145
Configuring IP Office for unsecured CTI connections.....	150
Configuring the Contact Center virtual machine.....	151
Configuring the virtual machine automatic startup settings.....	152
Chapter 10: Deploying Avaya Workspaces on Avaya Contact Center Select Software Appliance.....	155
Deploying the Avaya Workspaces OVA.....	156
Configuring Avaya Workspaces during the initial installation.....	158
Adding Avaya Workspaces to an existing solution.....	161
Part 3: User Contact Recording configuration.....	163
Chapter 11: User Contact Recording Pause and Resume configuration.....	164
Using IP Office Manager.....	164
Configuring a Pause Recording button for users.....	166
Configuring the Contact Recording Auto Restart Delay.....	170
Saving the IP Office configuration data.....	172
Part 4: Reverse proxy for Avaya Workspaces.....	173
Chapter 12: Solution overview.....	174
Supported contact types.....	174
Architecture overview.....	175
Prerequisites.....	176

Reverse proxy configuration process flow.....	176
Configuration and deployment details.....	177
Documentation of FQDNs and IP addresses of solution interfaces.....	178
Publishing of FQDNs external to the enterprise for remote agents.....	178
Function and role of the external firewall for remote agents.....	178
Function and role the reverse proxy for remote agents.....	179
Reverse proxy policies, TLS profiles, and relay services.....	179
Function and role of the internal firewall.....	179
Connectivity details of remote agents.....	180
Remote worker phone set configuration.....	180
Chapter 13: Avaya Session Border Controller for Enterprise configuration.....	181
Configuring Avaya SBCE networks.....	181
Creating a reverse proxy policy.....	182
Deploying Identity Certificate on Avaya SBCE.....	182
Creating the common client certificate.....	182
Creating the common server certificate.....	183
Creating a client profile for the Avaya Workspaces reverse proxy.....	184
Creating a server profile for the Avaya Workspaces reverse proxy.....	185
Extracting the certificate and private key in Session Border Controller.....	185
Installing the client and server certificates on Session Border Controller.....	186
Chapter 14: Configuring reverse proxy for Avaya Workspaces.....	187
Checklist for configuring reverse proxy for Avaya Workspaces.....	187
Documentation of Avaya Workspaces configuration details.....	188
Configuring a TLS server profile.....	189
Configuring a TLS client profile.....	190
Creating a reverse proxy relay service for Avaya Workspaces	191
Part 5: First phone call and first email.....	193
Chapter 15: Agent Desktop.....	194
Agent Desktop User Interface.....	194
Work Item paradigm.....	195
Top bar.....	195
Work list window.....	196
Action bar.....	197
Email User Interface.....	198
Installing Agent Desktop software using ClickOnce.....	199
Logging on to Agent Desktop.....	200
Changing your status to Ready.....	204
Making a test phone call to the contact center.....	204
Accepting a call.....	205
Entering an Activity code.....	206
Ending a call.....	206
Making a call.....	207
Sending a test email message to the contact center.....	207

Accepting an incoming email message.....	208
Replying to an email message.....	209
Logging off from Agent Desktop.....	211
Part 6: Maintenance	213
Chapter 16: Maintenance procedures	214
Adding a server to a domain.....	214
Backing up the Contact Center databases.....	215
Creating a backup location for scheduled backups.....	217
Scheduling a backup of the Contact Center server databases	218
Downloading the latest product documentation.....	220
Installing the most recent supported operating system service packs.....	220
Verifying if installed patches are up-to-date.....	221
Downloading the most recent Contact Center patches to the server.....	221
Disabling Windows Server Automatic Maintenance.....	222
Installing Contact Center patches.....	222
Enabling Windows Server Automatic Maintenance	223
Logging on to Avaya Aura [®] Media Server Element Manager.....	224
Backing up the Avaya Aura [®] Media Server software appliance database.....	225
Installing Avaya Aura [®] Media Server patches	226
Starting or stopping Contact Center server services.....	227
Rebooting the Avaya Aura [®] Media Server virtual machine.....	229
Shutting down the Avaya Aura [®] Media Server virtual machine.....	229
Part 7: Customization	230
Chapter 17: Customizing the solution	231
Configuring Internet Explorer.....	232
Accessing CCMA using Microsoft Edge with Internet Explorer mode.....	234
Adding the Microsoft Edge administrative templates.....	234
Configuring Internet Explorer integration.....	235
Configuring the Enterprise Mode Site List.....	236
Internet Explorer mode and Compatibility View configuration on the domain server.....	238
Adding the Microsoft Edge administrative templates to the domain server.....	239
Creating a configuration file for IE mode.....	240
Uploading the configuration file for IE mode to the CCMA server.....	242
Enabling IE mode on the domain server.....	243
Completing IE mode configuration on a local computer.....	244
Configuring Compatibility View settings on the domain server.....	245
Disabling Internet Explorer 11 as a standalone browser.....	246
Starting the Script Variables tool in Contact Center Manager Administration.....	247
Checking variables for referencing applications.....	248
Configuring business and public holiday dates.....	248
Configuring the office hours.....	250
Changing the default voice mail number.....	251

Changing the voice prompt audio files.....	253
Chapter 18: Avaya Contact Center Select users	255
Logging on to Contact Center Manager Administration	256
Creating a new agent.....	256
Updating agent details.....	259
Copying agent properties.....	260
Part 8: Agent Desktop	262
Chapter 19: Agent Desktop software installation	263
Installing Agent Desktop software using ClickOnce.....	263
Agent Desktop client software silent installation.....	264
Installing software prerequisites for an Agent Desktop silent install.....	265
Installing Agent Desktop client software silently.....	265
Part 9: Reporting	267
Chapter 20: Real Time Reporting	268
Using the Contact Center Status real-time display.....	268
Part 10: Troubleshooting	271
Chapter 21: Troubleshooting tips	272
Troubleshooting by symptom.....	273
Starting the Contact Center Dashboard.....	275
Verifying the Contact Center services are started.....	280
Checking that the SIP User Extension Number is acquired on IP Office.....	286
Checking the Contact Center connection to IP Office.....	288
Checking the Contact Center License Manager real time usage.....	289
Using the CCMM dashboard.....	290
Troubleshooting Contact Recording.....	291
Chapter 22: Avaya Workspaces troubleshooting	295
Prerequisites for Avaya Workspaces troubleshooting.....	295
Logging on to the Avaya Workspaces nodes after deployment.....	295
Troubleshooting error messages when deploying Avaya Workspaces OVA.....	296
Troubleshooting agent login failures.....	296
Restarting the Avaya Workspaces cluster on virtual solutions.....	297
Restarting an Avaya Workspaces container on virtual solutions.....	297
Troubleshooting “helm ls” health check command.....	298
Troubleshooting “kubectl get pods --all-namespaces” health check command.....	298
Troubleshooting Avaya Workspaces using the Avaya Workspaces Service Utility.....	298
Viewing containers.....	299
Viewing logs.....	299
Collecting logs.....	300
Appendix A: VMware Best Practices	302
VMware Best Practices for performance.....	302
Virtualization host hardware settings.....	302

VMware networking best practices.....	303
VMware Tools.....	304
Network Time Protocol and time configuration.....	304
Troubleshooting VMware.....	304

Chapter 1: Introduction

This document describes how to deploy, commission, and test the Avaya Contact Center Select Release 7.1 software appliance.

Purpose

This document describes how to install and commission Avaya Contact Center Select.

Intended audience

This document is intended for personnel who install Avaya Contact Center Select.

Related resources

The following are some additional Avaya Contact Center Select related resources.

Avaya Contact Center Select Documentation

The following table lists the documents related to Avaya Contact Center Select. Download the documents from the Avaya Support website at <http://support.avaya.com>.

Title	Use this document to:	Audience
Overview		

Table continues...

Title	Use this document to:	Audience
<i>Avaya Contact Center Select Solution Description</i>	This document provides a technical description of Avaya Contact Center Select. It describes the product features, specifications, licensing, and interoperability with other supported products.	Customers and sales, services, and support personnel
<i>Avaya Contact Center Select Documentation Catalog</i>	This document describes available Avaya Contact Center Select documentation resources and indicates the type of information in each document.	Customers and sales, services, and support personnel
<i>Contact Center Performance Management Data Dictionary</i>	This document contains reference tables that describe the statistics and data in the historical and real-time reports generated in Contact Center.	System administrators and contact center supervisors
Implementing		
<i>Deploying Avaya Contact Center Select DVD</i>	This document contains information about Avaya Contact Center Select DVD installation, initial configuration, and verification. This document contains information about maintaining and troubleshooting the Avaya Contact Center Select server.	Implementation personnel
<i>Deploying Avaya Contact Center Select Software Appliance</i>	This document contains information about Avaya Contact Center Select Software Appliance (VMware) preparation, deployment, initial configuration, and verification. This document contains information about maintaining and troubleshooting the software appliance.	Implementation personnel
<i>Deploying Avaya Contact Center Select Hardware Appliance</i>	This document contains information about Avaya Contact Center Select Hardware Appliance (physical server) installation, initial configuration, and verification. This document contains information about maintaining and troubleshooting the hardware appliance.	Implementation personnel
<i>Deploying Avaya Contact Center Select on Microsoft Azure</i>	This document contains information about deploying Avaya Contact Center Select using an ISO image on Microsoft Azure.	Implementation personnel
<i>Avaya Contact Center Select Business Continuity</i>	This document contains information about deploying Avaya Contact Center Select Business Continuity.	Implementation personnel

Table continues...

Title	Use this document to:	Audience
<i>Upgrading and patching Avaya Contact Center Select</i>	This document contains information about upgrading and patching Avaya Contact Center Select.	Implementation personnel and system administrators
Administering		
<i>Administering Avaya Contact Center Select</i>	This document contains information and procedures to configure the users, skillsets, and contact center configuration data. This document contains information about creating Avaya Contact Center Select real-time and historical reports.	System administrators and contact center supervisors
<i>Avaya Contact Center Select Advanced Administration</i>	This document contains information about managing the Avaya Contact Center Select server, licensing, and multimedia configuration.	System administrators
<i>Using Contact Center Orchestration Designer</i>	This document contains information and procedures to configure script and flow applications in Contact Center Orchestration Designer.	System administrators
Maintaining		
<i>Contact Center Event Codes</i>	This document contains a list of errors in the Contact Center suite and recommendations to resolve them. This document is a Microsoft Excel spreadsheet.	System administrators and support personnel
Using		
<i>Using Agent Desktop for Avaya Contact Center Select</i>	This document provides information and procedures for agents who use the Agent Desktop application to accept, manage, and close contacts of all media types in Contact Center.	Contact center agents and supervisors
<i>Using the Contact Center Agent Browser application</i>	This document provides information and procedures for agents who use the Agent Browser application to log on to Contact Center and perform basic tasks.	Contact center agents
<i>Using Avaya Workspaces for AACC and ACCS</i>	This document describes the tasks that Contact Center agents can perform using Avaya Workspaces.	Contact center agents and supervisors

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to <https://support.avaya.com/> and do one of the following:
 - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Content Type**.
 - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
 - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
 - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.

 **Note:**

Videos are not available for all products.

Support

Go to the Avaya Support website at <https://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: Changes in this release

The following sections describe the new features and changes in the Avaya Contact Center Select Release 7.1 deployment process.

Features

See the following sections for information about feature changes.

New features in the Release 7.1 base build

See the following sections for information about new features in the Release 7.1 base build:

[Avaya Contact Center Select Release 7.1 supports Microsoft Windows Server 2016](#) on page 18

[Ignition Wizard enhancements](#) on page 18

[Support for Avaya Workspaces](#) on page 19

New features in Release 7.1 Service Pack 1

There are no new features in Release 7.1 Service Pack 1.

New features in Release 7.1 Service Pack 2

There are no new features in Release 7.1 Service Pack 2.

New features in Release 7.1 Service Pack 3

See the following sections for information about new features in Release 7.1 Service Pack 3:

[Avaya Workspaces Service Utility](#) on page 18

New features in Release 7.1 Feature Pack 1

See the following sections for information about new features in Release 7.1 Feature Pack 1:

[NTP configuration of the Avaya Workspaces nodes](#) on page 19

New features in Release 7.1 Feature Pack 2

See the following sections for information about new features in Release 7.1 Feature Pack 2:

[Ability to deploy Avaya Workspaces at any stage](#) on page 17

[Contact Center Manager Administration supported in Microsoft Edge with IE mode](#) on page 18

[Microsoft Edge support in Agent Desktop](#) on page 18

[Support of reverse proxy for Avaya Workspaces](#) on page 19

New features in Release 7.1 Feature Pack 2 Post GA Patches

See the following sections for information about new features in Release 7.1 Feature Pack 2 Post GA Patches:

[Avaya Contact Center Select Release 7.1 Feature Pack 2 Post GA Patches supports Microsoft Windows 11](#) on page 17

[Avaya Contact Center Select Release 7.1 Feature Pack 2 Post GA Patches supports Microsoft Windows Server 2019](#) on page 17

Ability to deploy Avaya Workspaces at any stage

From Release 7.1 Feature Pack 2, you can deploy and configure the Avaya Workspaces cluster at any stage after you upgrade to the latest release. Using the Update Configurator, you can deploy the Avaya Workspaces cluster either during initial installation and configuration of the Contact Center release, or as a Day 2 operation.

Avaya Contact Center Select Release 7.1 Feature Pack 2 Post GA Patches supports Microsoft Windows 11

From Release 7.1 Feature Pack 2 Post GA Patches, Avaya Contact Center Select supports Microsoft Windows 11 for Avaya Agent Desktop, Contact Center Manager Administration, Contact Center Multimedia Administration, and Communication Control Toolkit.

Avaya Contact Center Select Release 7.1 Feature Pack 2 Post GA Patches supports Microsoft Windows Server 2019

Avaya Contact Center Select Release 7.1 Feature Pack 2 Post GA Patches supports the Microsoft Windows Server 2019 operating system. Customers that upgrade to Avaya Contact Center Select Release 7.1 Feature Pack 2 Post GA Patches and want to use Windows Server 2019 must perform a fresh installation on a new Microsoft Windows Server 2019. For more information about restoring the database to the new server, see *Upgrading and patching Avaya Contact Center Select*.

Avaya Contact Center Select Release 7.1 supports Microsoft Windows Server 2016

Avaya Contact Center Select Release 7.1 is supported on both the Microsoft Windows Server 2012 R2 and Microsoft Windows Server 2016 operating system. Customers upgrading to Avaya Contact Center Select 7.1 on Windows Server 2016, must migrate to a new Microsoft Windows Server 2016 server.

Avaya Workspaces Service Utility

From Release 7.1, Service Pack 3, you can use Avaya Workspaces Service Utility — a new standalone .NET application to perform service functions for Workspaces cluster. You can use this tool to monitor the containers and collect logs.

Contact Center Manager Administration supported in Microsoft Edge with IE mode

From Release 7.1 Feature Pack 2, you can access Contact Center Manager Administration using Microsoft Edge with Internet Explorer (IE) mode.

Ignition Wizard enhancements

From Release 7.1 the following enhancements of Ignitions Wizard are implemented:

- Ignition Wizard now supports chained certificates
 - Ignition Wizard now allows to remove the imported certificates
 - Password complexity rules of Ignition Wizard are now aligned with Security Manager
 - Ignition Wizard now has enhanced validation and reset options
-

Microsoft Edge support in Agent Desktop

From Release 7.1 Feature Pack 2, Agent Desktop uses the Microsoft Edge browser as a rendering engine to display web content. To display sites that are compatible only with Internet Explorer, you must enable IE mode for Agent Desktop using new functionality in Contact Center Multimedia Administration. This feature requires installation of Microsoft Edge WebView2 Runtime.

You can also install and start Agent Desktop using Microsoft Edge.

NTP configuration of the Avaya Workspaces nodes

From Release 7.1 Feature Pack 1, you can synchronize your Avaya Workspaces nodes with the Contact Center environment using Network Time Protocol (NTP) servers. Set up the NTP servers before deploying or upgrading your Contact Center Release 7.1. You can use from one to three NTP servers, however, Avaya recommends that you use three. You can configure time synchronization settings in the new Other settings tab while configuring Avaya Workspaces in Ignition Wizard (for fresh installs) or in the Update Configurator (for upgrades).

Support for Avaya Workspaces

From Release 7.1 Contact Center supports Avaya Workspaces — a client for voice, email and webchat contact types.

Support of reverse proxy for Avaya Workspaces

From Release 7.1 Feature Pack 2, Contact Center introduces support for reverse proxy, which allows agents to access Avaya Workspaces from outside the corporate network without VPN connection. You can configure reverse proxy for Avaya Workspaces using Avaya Session Border Controller for Enterprise.

Other changes

See the following sections for information about changes that are not feature-related:

Other changes in the Release 7.1 base build

See the following sections for information about new features in the Release 7.1 base build:

[Avaya Aura Media Server update](#) on page 20

[Support for VMware 6.7](#) on page 21

Other changes in Release 7.1 Service Pack 1

There are no other changes in Release 7.1 Service Pack 1.

Other changes in Release 7.1 Service Pack 2

There are no other changes in Release 7.1 Service Pack 2.

Other changes in Release 7.1 Service Pack 3

There are no other changes in Release 7.1 Service Pack 3.

Changes in this release

Other changes in Release 7.1 Feature Pack 1

See the following sections for information about other changes in Release 7.1 Feature Pack 1:

[Avaya Aura Media Server update](#) on page 20

[Support for the latest WebLM release](#) on page 21

[Updated third-party software for the Avaya Workspaces cluster](#) on page 21

Other changes in Release 7.1 Feature Pack 2

See the following sections for information about other changes in Release 7.1 Feature Pack 2:

[Avaya Aura Media Server update](#) on page 20

[Documentation update for Avaya Workspaces deployment](#) on page 20

[Support for VMware version 7.0](#) on page 21

[Updated third-party software for the Avaya Workspaces cluster](#) on page 21

Avaya Aura® Media Server update

Contact Center Release 7.1 supports Avaya Aura® Media Server Release 8.0. Avaya Aura® Media Server Release 8.0 is supported on the Red Hat Enterprise Linux 7.x 64-bit operating system only.

Avaya Aura® Media Server update

From Release 7.1 Feature Pack 1, Contact Center supports Avaya Aura® Media Server Release 8.0.2 SP3 and SP4.

Avaya Aura® Media Server update

From Release 7.1 Feature Pack 2, Contact Center supports Avaya Aura® Media Server Release 8.0.2 SP7.

Documentation update for Avaya Workspaces deployment

From Release 7.1 Feature Pack 2, the Avaya Workspaces deployment chapter has been added to *Deploying Avaya Contact Center Select Software Appliance*. The new chapter provides more detailed information about installing Avaya Workspaces during the initial installation of Avaya Contact Center Select and adding Avaya Workspaces to an existing solution. See [Deploying Avaya Workspaces on Avaya Contact Center Select Software Appliance](#) on page 155.

Support for VMware 6.7

From Release 7.1 Contact Center supports VMware 6.7. Contact Center Release 7.1 continues supporting the previous versions of VMware 6.7, as well as the same features of previous releases.

Support for VMware version 7.0

From Release 7.1 Feature Pack 2, Contact Center supports VMware version 7.0 . Contact Center continues to support VMware version 6.5 and 6.7.

Support for the latest WebLM release

From Release 7.1 Feature Pack 1, Contact Center supports WebLM 8.1.2.

Updated third-party software for the Avaya Workspaces cluster

Release 7.1 Feature Pack 1 upgrades a number of third-party components for the Avaya Workspaces cluster to recent versions, such as Kubernetes, Docker, Istio, and Kafka.

Updated third-party software for the Avaya Workspaces cluster

Release 7.1 Feature Pack 2 upgrades a number of third-party components for the Avaya Workspaces cluster to recent versions, such as Kubernetes, Docker, Istio, and Kafka.

Chapter 3: Overview

For increased productivity, efficiency, and flexibility, Avaya Contact Center Select supports VMware virtualization.

Avaya Contact Center Select offers a software appliance package that consists of the following components:

- Avaya Contact Center Select virtual machine
- Avaya Aura[®] Media Server OVA
- Avaya WebLM OVA
- Optional Avaya Workspaces — one additional Avaya Workspaces node, deployed using the Avaya Workspaces Open Virtual Appliance (OVA)

You can use a single Open Virtual Appliance (OVA) package to distribute a virtual appliance. For example, an Avaya Aura[®] Media Server OVA package includes all of the Open Virtualization Format (OVF) information required to create an Avaya Aura[®] Media Server virtual appliance on a VMware host. A virtual appliance contains a preinstalled, preconfigured operating system and an application stack optimized to provide a specific set of services. The Avaya Aura[®] Media Server and Avaya WebLM OVAs are prepackaged and ready for deployment.

For the Avaya Contact Center Select virtual machine, you must build a suitably specified virtual machine and then install product software from the Avaya Contact Center Select DVD or ISO image.

The following diagram shows a typical virtualized contact center solution using Avaya Contact Center Select, Avaya Aura[®] Media Server, and Avaya WebLM deployed on a single VMware host server.

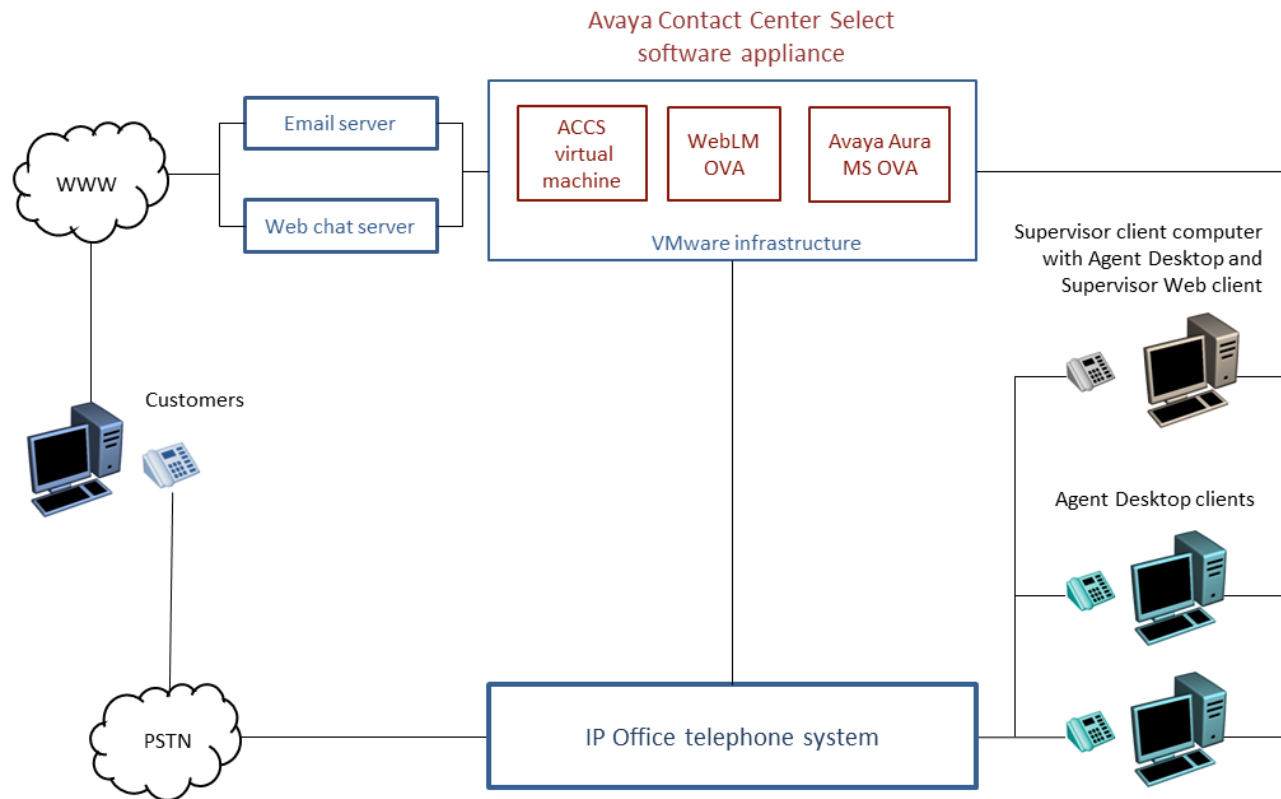


Figure 1: Avaya Contact Center Select virtualized contact center solution with Avaya Aura® Media Server and Avaya WebLM

You can use VMware vSphere or vCenter and these components to create virtual machines in your virtualized environment. The OVA packages are created as VMware hardware version 8 archives.

Avaya Contact Center Select supports the following virtualization environments:

- ESXi 6.0
- ESXi 6.5
- ESXi 6.7
- ESXi 7.0

! Important:

- Avaya Workspaces is supported on ESXi 6.5 and later.
- Avaya Contact Center Select on Windows Server 2016 and Windows Server 2019 is supported on ESXi 6.5 and later.
- VMFS 5.54 or later is required for all supported versions of ESXi.

Avaya Contact Center Select supports the Avaya WebLM virtual machine co-resident on the same VMware host server or deployed on a separate VMware host server.

Overview

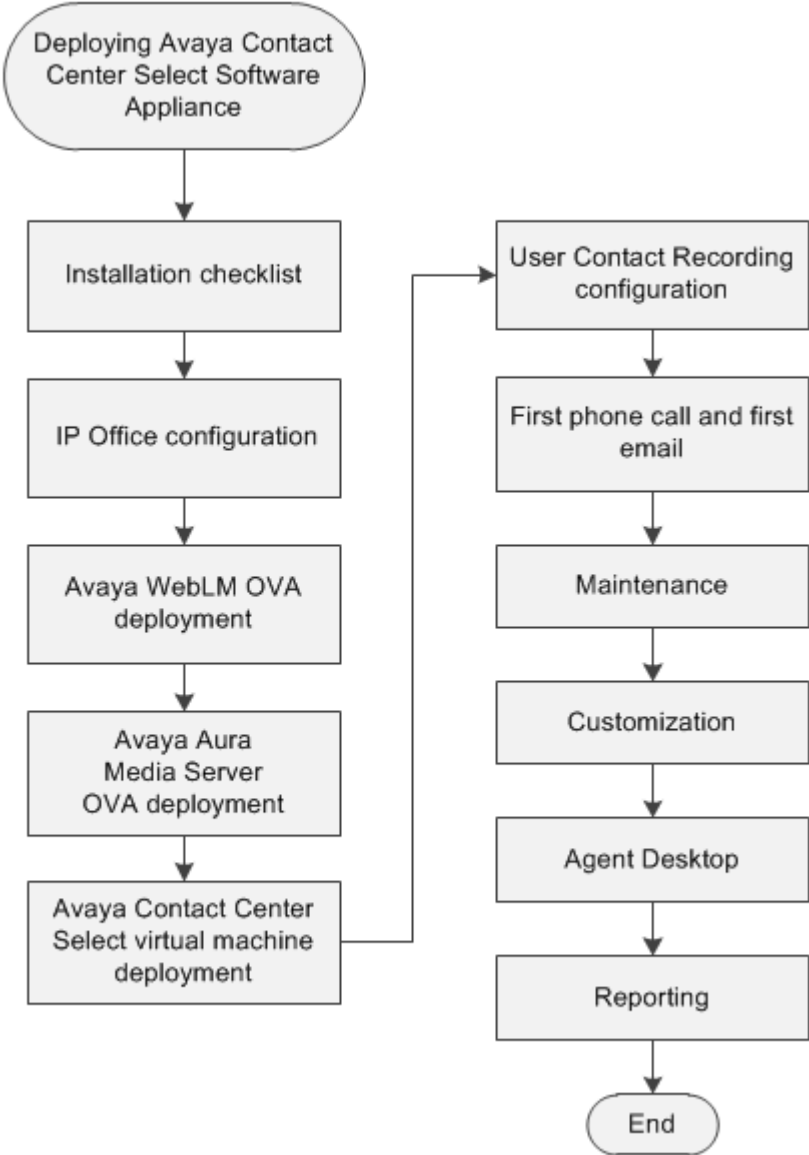
Avaya Contact Center Select supports the Avaya Aura® Media Server virtual machine co-resident on the same VMware host server or deployed on a separate VMware host server.

Avaya Contact Center Select supports the Avaya Workspaces virtual machine co-resident on the same VMware host server or deployed on a separate VMware host server.

The Avaya Contact Center Select server is supported in a workgroup or in a Windows domain. After you deploy Avaya Contact Center Select, you can add the server to a Windows domain.

Chapter 4: Deployment process

This work flow shows the sequence of tasks you perform to deploy Avaya Contact Center Select.



Chapter 5: Installation checklist

The following sections list the main Avaya IP Office, Avaya WebLM, Avaya Aura® Media Server, and Avaya Contact Center Select configuration and deployment details. You must know these configuration details before you can deploy and commission an Avaya Contact Center Select solution.

Complete these checklists before continuing.

Avaya IP Office configuration checklist

The following table lists and describes the configuration details required by IP Office.

Configuration Item	Your value	Description
IP Office Server type		Is the IP Office a Server Edition server.
Server release		The IP Office software release.
IP address		The IP address of the IP Office server.
IP Office System Password		In IP Office Manager, select <i>File > Advanced > Security Settings</i> . Select <i>System</i> and then select the <i>Unsecured Interfaces</i> tab. The IP Office System Password is configured here.
IP Office Manager IP address		The IP address of the client computer with IP Office Manager software.
IP Office Manager user name		The user name used to log on to IP Office Manager.
IP Office Manager password		The password used to log on to IP Office Manager.
Avaya Contact Center Select IP address		The IP address of the Avaya Contact Center Select server.
Avaya Contact Center Select username		The name of the Avaya Contact Center Select data synchronization user account. The default user name is accssync.
Avaya Contact Center Select password		The password of the Avaya Contact Center Select data synchronization user account. The default password is accssync.

Table continues...

Configuration Item	Your value	Description
SIP domain name		The name of the SIP domain used by IP Office.
SIP User Extension Number		The IP Office SIP User Extension Number used by Avaya Contact Center Select to register for CTI call control and SIP session messaging.
SIP User Extension Password		A password for the IP Office SIP User Extension Number. The password must be a number.
SIP User Login Code [User > Telephony > Supervisor Settings > Login Code]		The IP Office SIP User Telephony Supervisor Login Code used by Avaya Contact Center Select to register for CTI call control and SIP session messaging. The Login Code must be a number.
Short Code – Code number		A solution short code to map an IP Office telephone number to the Avaya Contact Center Select SIP User Extension Number.
Short Code - Telephone Number		A short code telephone number that outputs to an Avaya Contact Center Select CDN (Route Point).
Agent extensions		The IP Office Extensions to be used by Avaya Contact Center Select users.

Avaya WebLM deployment checklist

The following table lists and describes the configuration details required by WebLM.

Configuration Item	Your value	Description
Virtual machine name in VMware inventory		The name of the WebLM virtual machine as it appears on the VMware inventory list.
Server hostname		The host name of the WebLM server
Server IP address		The IP address of the WebLM server.
Server mask		The network mask of the WebLM server.
Server domain name		The domain the WebLM server is on.
Server default gateway		The default gateway used by the WebLM server.
DNS server IP address		The IP address of the DNS server used by the WebLM server.
WebLM User Name		The user name used to log on to the WebLM web interface.
WebLM Password		The password used to log on to the WebLM web interface.
Primary Host ID		The WebLM server Host ID used to obtain a license.

Avaya Aura[®] Media Server deployment checklist

The following table lists and describes the configuration details required by Avaya Aura[®] Media Server.

Configuration Item	Your value	Description
Virtual machine name in VMware inventory		The name of the Avaya Aura [®] Media Server virtual machine as it appears on the VMware inventory list.
Server hostname		The host name of the Avaya Aura [®] Media Server Linux server.
IP address		The IP address of the Avaya Aura [®] Media Server server.
Network Mask		The network mask of the Avaya Aura [®] Media Server server.
Default Gateway IP address		The default gateway used by the Avaya Aura [®] Media Server server.
DNS server IP address		The IP address of the DNS server used by Avaya Aura [®] Media Server.
NTP server IP address		The IP address for the Network Time Protocol (NTP) server.
Administration account "Admin123\$" password		A password for the Avaya Aura [®] Media Server Element Manager interface.

Avaya Contact Center Select deployment checklist

The following table lists and describes the configuration details required by Avaya Contact Center Select. The email related configuration items are optional.

Configuration Item	Your value	Description
Virtual machine name in VMware inventory		The name of the Avaya Contact Center Select virtual machine as it appears on the VMware inventory list.
Server hostname		<p>The host name of the Avaya Contact Center Select server.</p> <p>Server names must adhere to RFC1123. For more information, see <i>Avaya Contact Center Select Solution Description</i>.</p> <p>Avaya recommends that you configure the server final production name when installing Avaya Contact Center Select.</p>

Table continues...

Configuration Item	Your value	Description
Server IP address		The IP address of the Avaya Contact Center Select server.
Server mask		The network mask of the Avaya Contact Center Select server.
Server default gateway		The default gateway used by the Avaya Contact Center Select server.
DNS server IP address		The IP address of the DNS server used by Avaya Contact Center Select.
Country or region		The Microsoft Windows Server country or region server setting.
Time and currency		The Microsoft Windows Server time and currency server setting.
Keyboard layout		The Microsoft Windows Server keyboard layout server setting.
Microsoft Windows Server Standard or Datacenter edition product key		The Microsoft Windows Server Standard or Datacenter edition product key used to activate the Operating System.
Administrator password		A password for the Avaya Contact Center Select server.
IP Office Server - IP Address		The IP address of the IP Office server.
IP Office Server - Voice Port		The number of the voice port used to communicate with IP Office. The default port number is 5060.
IP Office SIP Domain Name		The name of the SIP Domain used by IP Office.
IP Office Service User - Username		The name of the IP Office data synchronization service user. Avaya Contact Center Select uses this IP Office service user for data synchronization with IP Office.
IP Office Service User - Password		The IP Office data synchronization service user password.
IP Office System Password		The System Password for the IP Office server.
Sample agent IDs		The phone number of the first IP Office sample user.
Voicemail Mailbox Number		The voice mail number used by the Customer Service sample application in Orchestration Designer.
Sample CDN (Route Point)		The phone number of the IP Office sort code Telephone Number.

Table continues...

Configuration Item	Your value	Description
Avaya Aura® Media Server IP Address		The IP Address of the Avaya Aura® Media Server.
Avaya Aura® Media Server Locale		The language and country locale used by Avaya Aura® Media Server.
System Account Configuration Password.		A password for the Avaya Contact Center Select administration account.
WebLM IP Address		The IP address of the WebLM server.
Mailbox Display Name		The display name of the Avaya Contact Center Select mailbox.
Mailbox email address		The email address of the Avaya Contact Center Select mailbox.
Mailbox email password		The password for the Avaya Contact Center Select mailbox.
Incoming Mail Server host name		The name of the server on which email messages are received in your network.
Incoming Mail Server protocol		The communication protocol for the inbound email server.
Incoming Mail Server encryption type		The encryption type used by the inbound email server.
Incoming Mail Server port number		The port number used by the inbound email server.
Outgoing Mail Server host name		The name of the server from which email messages are sent. Your inbound and outbound mail servers can have the same name.
Outgoing Mail Server protocol type		The communication protocol for the outbound email server.
Outgoing Mail Server encryption type		The encryption type used by the outbound email server.
Outgoing Mail Server port number		The port number used by the outbound email server.
Outgoing Mail Server SMTP Authentication type		The authentication type used by the outbound email server.

Avaya Workspaces installation checklist

The following table lists the main Avaya Workspaces configuration questions.

Configuration item	Your value	Description
Workspaces Cluster IP Address		The IP address of the Avaya Workspaces three-node cluster. You must use the Cluster IP Address to access the Avaya Workspaces cluster.

Table continues...

Configuration item	Your value	Description
Password		The root password to access the Avaya Workspaces nodes.
LDAP Server IP address		The IP address of your LDAP server.

The following table lists the main Network Time Protocol (NTP) servers questions.

Configuration Item	Your value	Description
NTP server IP address 1		The IP addresses of NTP servers. You must set up the NTP server(s) on site before installing or upgrading your Contact Center. You can use from one to three NTP servers, however, Avaya recommends that you use three NTP servers. The NTP servers must be trusted and return the same time. For resiliency, ensure that your NTP servers reside on more than one host.
NTP server IP address 2		
NTP server IP address 3		

Part 1: IP Office configuration

Chapter 6: IP Office configuration

Configure IP Office to integrate with Avaya Contact Center Select. This section does not describe IP Office basic configuration for system settings, licensing, or networking. This section describes only how to integrate a working IP Office server with Avaya Contact Center Select.

The procedures in this section use examples to describe how to configure IP Office to integrate with Avaya Contact Center Select. The IP Office configuration values used in the following procedures match the default values used by Avaya Contact Center Select. These values might not be suitable for your solution. If you use different IP Office configuration values, remember to enter the different values when installing and commissioning Avaya Contact Center Select.

Avaya recommends that you configure IP Office before installing Avaya Contact Center Select.

You must complete the procedures in this IP Office section in sequential order.

IP Office supported versions

Each Avaya Contact Center Select connects to a single IP Office Server Edition Primary server. Avaya Contact Center Select Business Continuity-enabled solutions support connecting to an IP Office Secondary server. A Small Community Network (SCN) is a system of networked IP Office telephone systems that can share extension numbers and user names. Each IP Office SCN supports a single connected Avaya Contact Center Select. The Avaya Contact Center Select server and the connected IP Office server must be located at the same campus location.

To support an IP Office SCN, Avaya Contact Center Select must connect to an IP Office Server Edition Primary server in that SCN network.

Avaya Contact Center Select supports only the following versions of IP Office:

- IP Office Server Edition Release 10.1, or 11.x
- IP Office 500V2, Release 10.1, or 11.x software, Standard Mode, Advanced Edition license

Avaya Contact Center Select does not support other versions of IP Office. For more information about the supported IP Office versions, refer to the Avaya Contact Center Select Release Notes.

Avaya Contact Center Select does not support IP Office 500V2 Basic mode.

Using IP Office Manager

Before you begin

- Install the IP Office Manager software on a client computer.
- Ensure the client computer can communicate with the IP Office server.

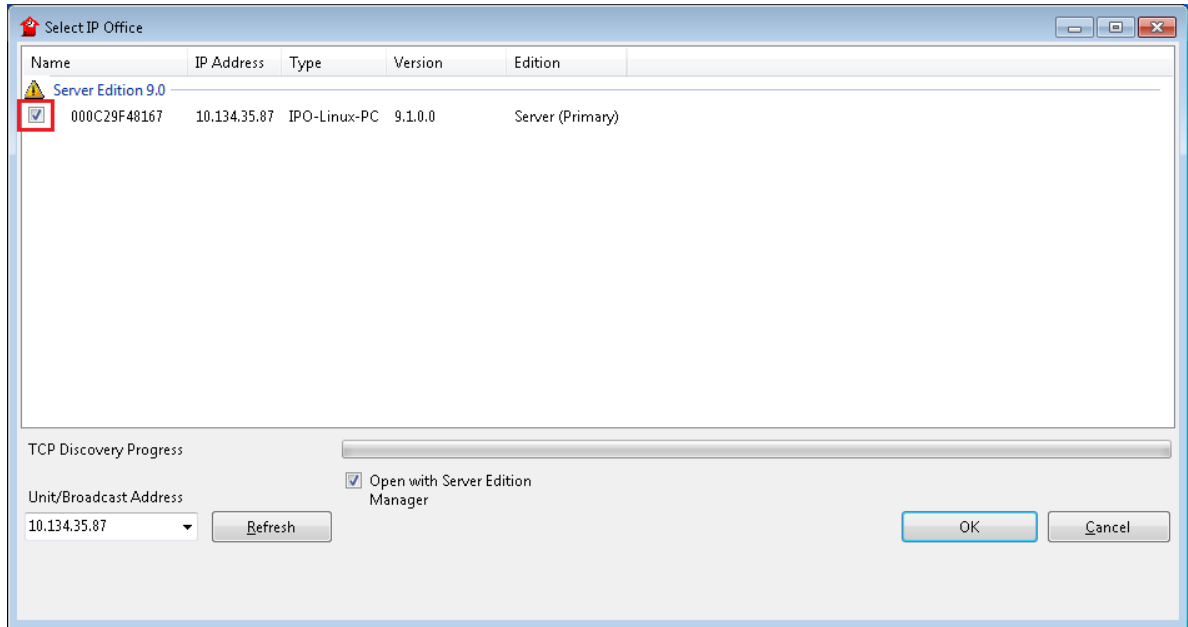
About this task

IP Office Manager is a component of the IP Office administration suite of applications. You use IP Office Manager to configure IP Office. IP Office Manager runs on a Windows computer and connects to the IP Office system using an Ethernet LAN connection.

IP Office Manager is an off-line editor. Use IP Office Manager to connect to your IP Office server and retrieve a local copy of the IP Office current configuration settings. You can then edit the local copy of the IP Office configuration and when you are ready, save your updated configuration data back to the IP Office server.

Procedure

1. On the client computer, select **Start > All Programs > IP Office > Manager**.
2. On the **Configuration Service User Login** message box, in the **Service User Name** box, type the user name. The default name is Administrator.
3. In the **Service User Password** box, type the user password. The default password is Administrator.
4. From the menu, select **File > Close Configuration**. This closes any open and potentially out-of-date configurations.
5. To retrieve the current (most recent) IP Office configuration settings, from the menu, select **File > Open Configuration**.
6. In the **Select IP Office** window:
 - If the required IP Office server is listed, use the check box to select your IP Office server from the list of available servers.
 - If the required IP Office server is not listed, in the **Unit/Broadcast Address** box type the IP address for your IP Office server. Click **Refresh** to perform a new search. The IP Office server then appears in the list of available servers. Use the check box to select your IP Office server from the list of available servers.



7. Click **OK**.
8. On the **Configuration Service User Login** message box, in the **Service User Name** box, type the user name. The default name is Administrator.
9. In the **Service User Password** box, type the user password. The default password is Administrator.
10. IP Office Manager opens and displays the current configuration data for your IP Office server.

Configuring the data synchronization user account

About this task

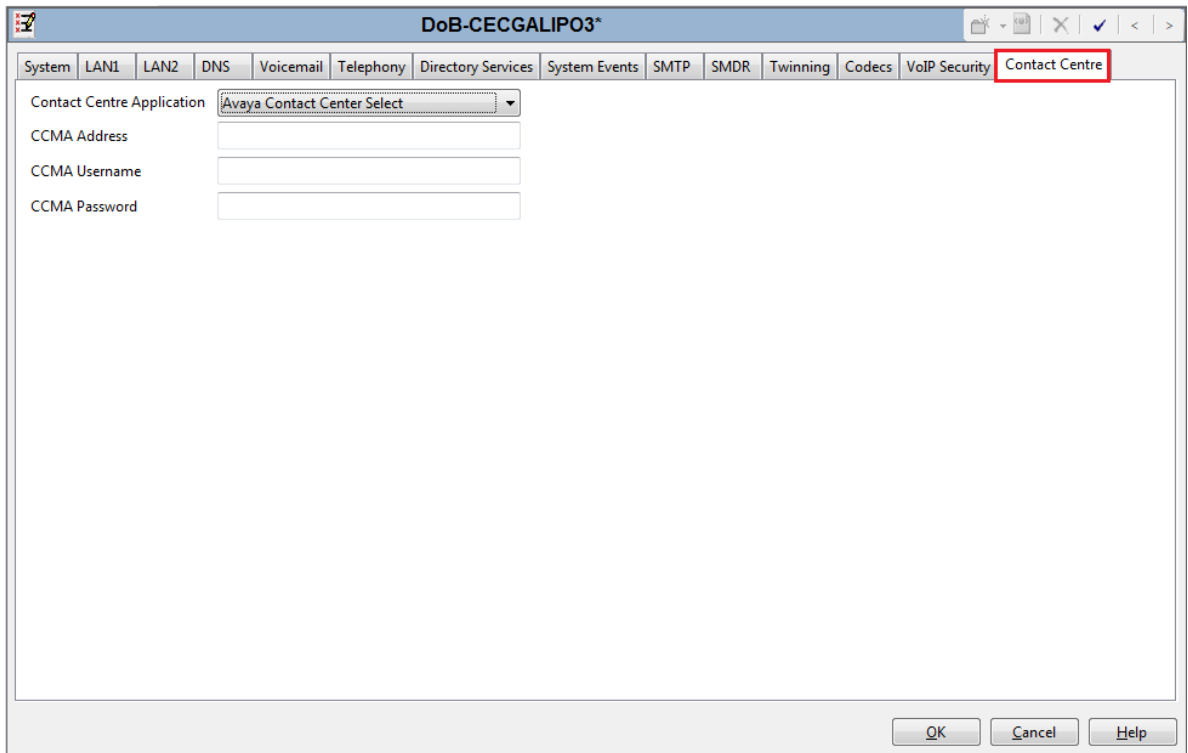
Configure the user account used by IP Office to maintain data synchronization with Avaya Contact Center Select.

For user data synchronization, IP Office connects to Avaya Contact Center Select using the Contact Center Manager Administration “accsync” user account details.

Procedure

1. Using IP Office Manager, select the IP Office server in the **Configuration** pane.
2. In the **Configuration** pane, under the IP Office server, select **System**.

3. Select the **Contact Center** tab.



4. From the **Contact Center Application** list, select Avaya Contact Center Select.
5. In the **CCMA Address** box, type the IP address of the Avaya Contact Center Select server. For example, type `http://1.2.3.4`

*** Note:**

If security is enabled on the Avaya Contact Center Select server, use HTTPS.

6. In the **CCMA Username** box, type the name of the Avaya Contact Center Select data synchronization user account. The default user name is `accsync`.
7. In the **CCMA Password** box, type the password of the Avaya Contact Center Select data synchronization user account. The default user password is `accsync`.
8. Click **OK**.

Configuring an IP Office service user for data synchronization

About this task

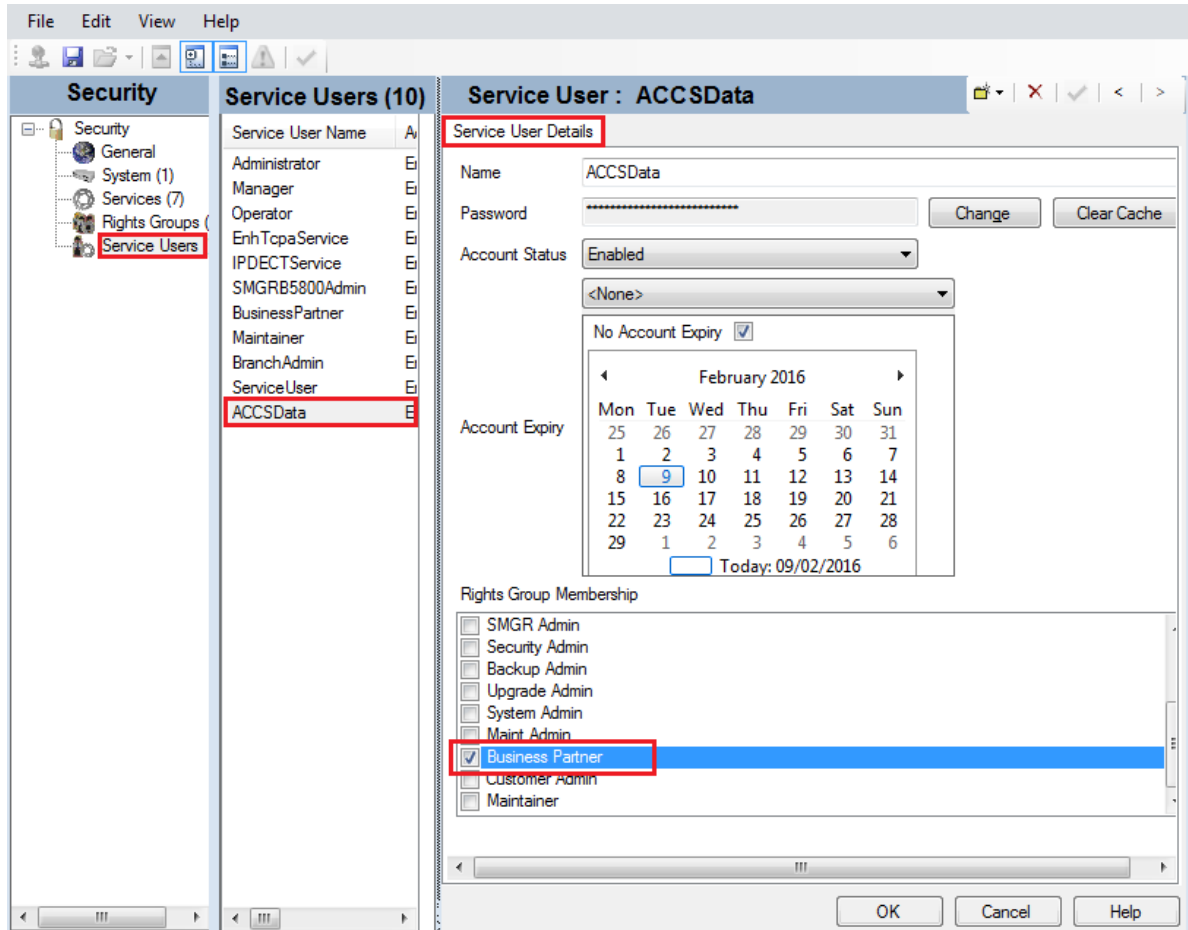
Create and configure an IP Office service user to support data synchronization with Avaya Contact Center Select.

Avaya Contact Center Select uses this IP Office service user account to synchronize agent and supervisor data between Avaya Contact Center Select and the IP Office platform.

Procedure

1. Log in to IP Office Manager with Administrator privileges.
2. Select **File > Advanced > Security Settings**.
3. On the **Service Users** list pane, right-click and select **New**.
4. On the **New Service User Details** screen, in the **New User Name** box, type the name for the new service user.
For example, ACCSData.
5. In the **New User Password** box, type the password for the new service user.
6. In the **Re-enter New User Password** box, re-type the password for the new service user.
7. Click **OK**.
8. On the **Service Users** list pane, select the new service user.

- On the **Service User Details** pane, from the **Rights Group Membership** list, select **Business Partner**.



- Click **OK**.
- Select **File > Save Security Settings**.

Verifying the IP Route configuration

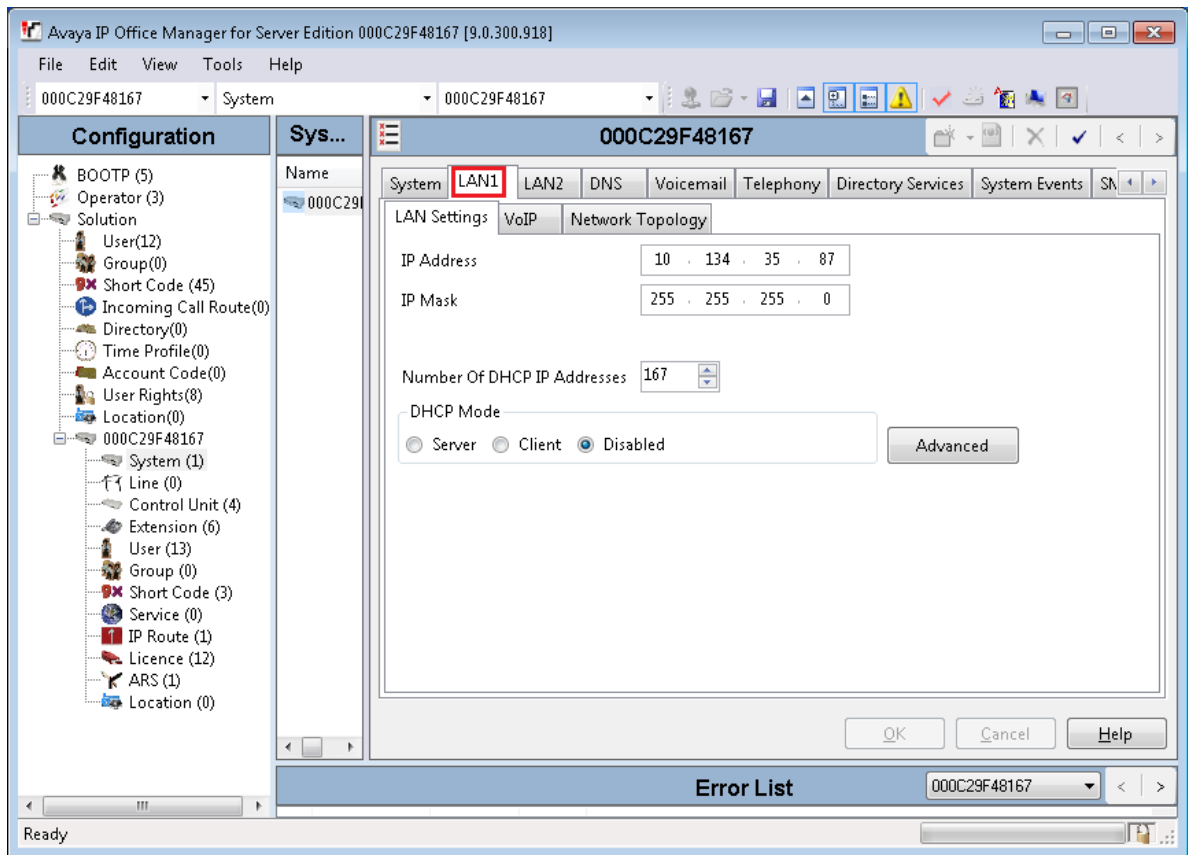
About this task

Verify the Local Area Network (LAN) Ethernet and IP Route configuration details to ensure IP Office can communicate with IP Office Manager, Avaya Contact Center Select, and agent telephones.

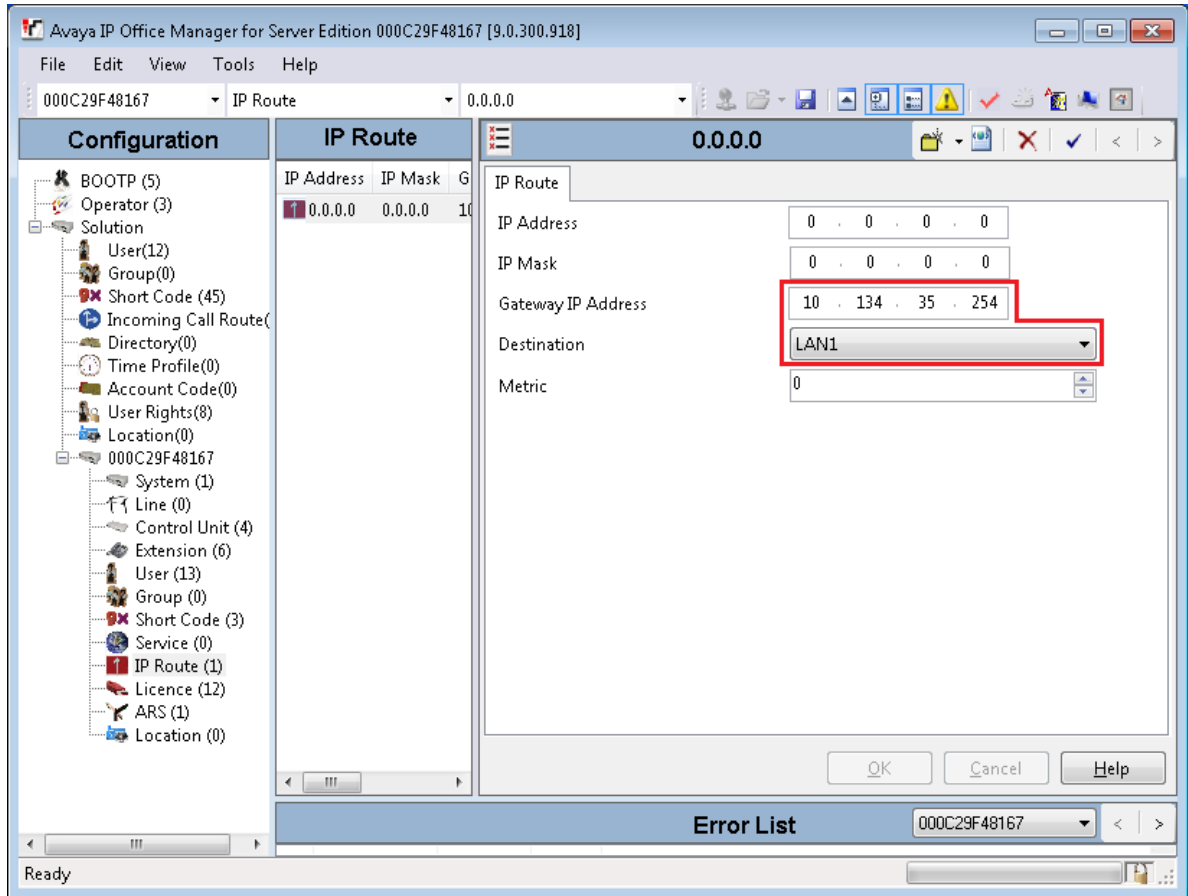
Procedure

- Using IP Office Manager, select the IP Office server in the **Configuration** pane.
- In the **Configuration** pane, under the IP Office server, select **System**.

- Note the IP Office network settings. Note which network interface IP Office is using for local communications. For Avaya Contact Center Select deployments, IP Office must use LAN1 for local communications.



- In the **Configuration** pane, under the IP Office server, select **IP Route**. If there are no existing IP Routes, right-click **IP Route** and select **New**.
- On the **IP Route** tab, in the **IP Address** box, type 0 . 0 . 0 . 0.
- In the **IP Mask** box, type 0 . 0 . 0 . 0.
- In the **Gateway IP Address** box, type the IP address of your gateway.
- From the **Destination** list, select the network interface that IP Office uses for local communication. For example, select LAN1.



9. Click **OK**.

Configuring the SIP domain name

About this task

Configure the IP Office SIP domain name. A SIP domain is a logical space where SIP-enabled devices exist, authenticate, register, and communicate.

In a SIP network a destination address consists of both a user and a domain. This is referred to as a Uniform Resource Identifier (URI). The user portion of the URI is the destination that is being communicated to and the domain portion is the logical grouping that the destination belongs to.

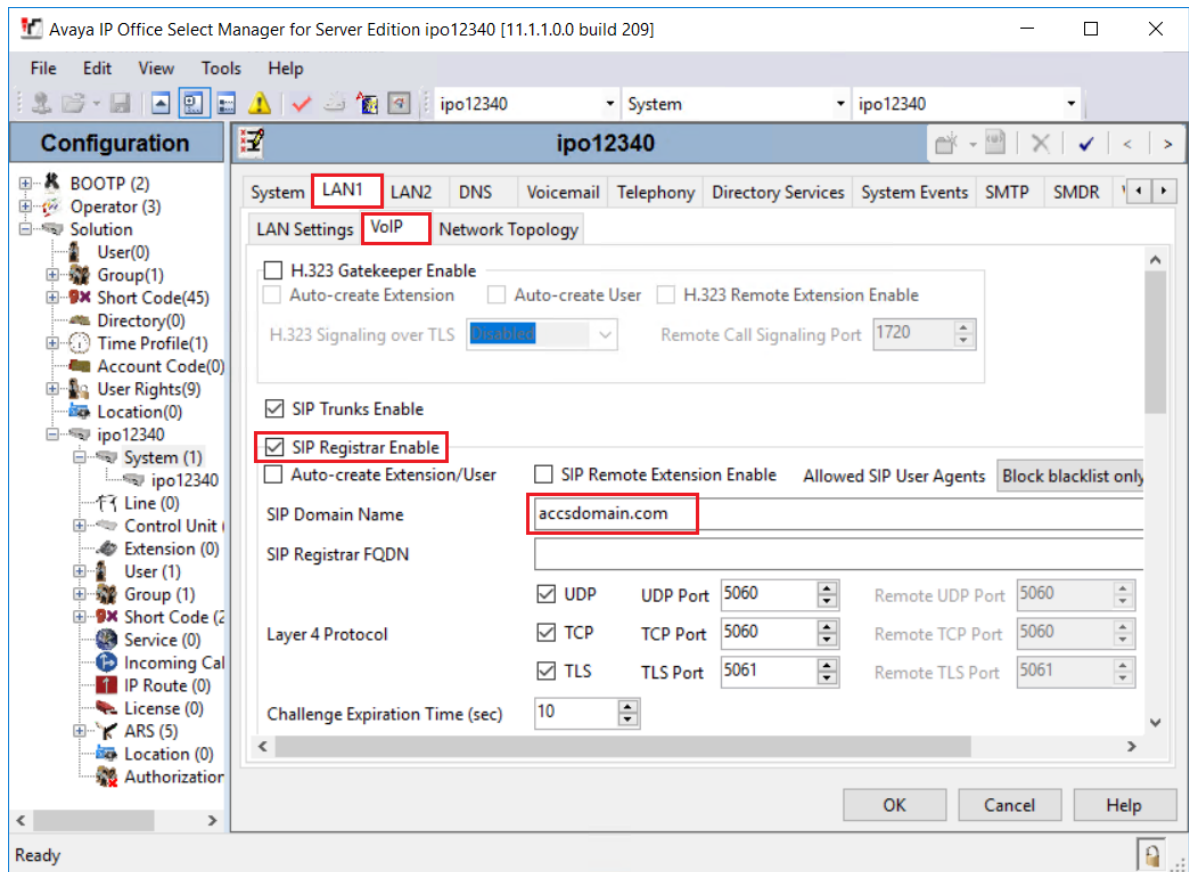
! Important:

If you add or change the domain name of an active IP Office server, the IP Office server restarts.

The Avaya Contact Center Select SIP domain name must match the IP Office SIP domain name.

Procedure

1. Using IP Office Manager, select the IP Office server in the **Configuration** pane.
2. In the **Configuration** pane, under the IP Office server, select **System**.
3. In the right pane, select the **LAN1** tab.
4. Select the **VoIP** tab.
5. Enable **SIP Registrar Enable**.
6. In the **Domain Name** box, type the name of the SIP domain to be used with Avaya Contact Center Select.



7. Click **OK**.

Configuring the SIP User Extension number

About this task

Configure an IP Office SIP User Extension number for desk phones and softphones. Avaya Contact Center Select uses this SIP User Extension number and Telephony Supervisor *Login Code* password to register for CTI call control and SIP session messaging.

Procedure

1. Using IP Office Manager, select the IP Office server in the **Configuration** pane.
2. In the **Configuration** pane, under the IP Office server, select **User**.
3. Right-click on **User**, and select **New**.
4. In the right pane, select the new **User** tab.
5. In the **Name** box, type a descriptive name for the user.
6. In the **Password** box, type a password for the user.

The password can be up to 31 alphanumeric characters long. Password complexity rules are set through the General security settings.

7. In the **Confirm Password** box, re-type a password for the user.
8. In the **Extension** box, type the extension number of the user. For example, type 6000.
For desk phones, the Extension value must match the Base Extension value of a phone. For more information, see [Configuring IP Office extensions](#) on page 48.
9. Select the **Telephony** tab.
10. On the **Telephony** tab, on the **Supervisor Settings** sub-tab, in the **Login Code** box, type a password for Avaya Contact Center Select registration. For example, type 123456. This password must be a number.
11. Click **OK**.
12. On the **Would you like a new VoIP extension created with this number** message box, select **SIP Extension** and click **OK**.

Configuring a short code for Contact Center Route Points

About this task

Configure a solution short code to map an IP Office telephone number to the Avaya Contact Center Select SIP User Extension Number. A short code configures IP Office to perform an action if a specific number is dialed.

For example:

- 3000 is configured in Avaya Contact Center Select as a CDN (Route Point).

- 6000 is configured in IP Office as the Avaya Contact Center Select SIP User Extension Number.

Create a short code 6000|>>3000. All customer calls to telephone number 3000 are forwarded to extension 6000 and from there to Avaya Contact Center Select. Avaya Contact Center Select can then treat the customer call and route it to a contact center agent.

This task describes a basic IP Office short code used to route calls to Avaya Contact Center Select. For information about implementing production grade short codes, refer to your IP Office documentation.

A CDN (Route Point) is a logical address used by Contact Center to accept incoming contacts or as a point to which contacts are routed. A Route Point is an address that enables incoming voice contacts (phone calls) to be treated by Contact Center.

You can add multiple short codes and configure each one to map to an Avaya Contact Center Select CDN (Route Point) number. If you create additional short codes to map IP Office calls to Avaya Contact Center Select, you must add the corresponding CDN (Route Point) number in Contact Center Manager Administration on the Avaya Contact Center Select server.

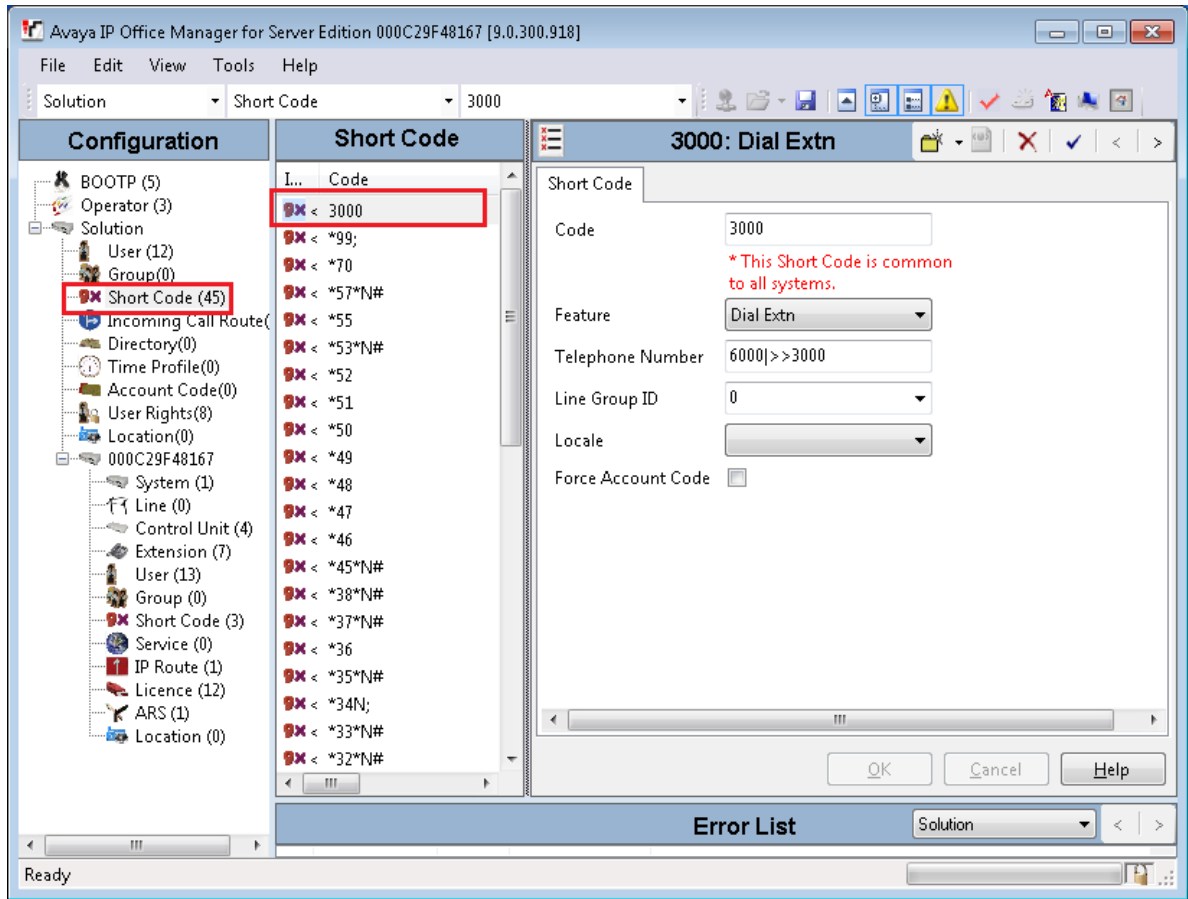
Procedure

1. Using IP Office Manager, select the IP Office server in the **Configuration** pane.
2. In the **Configuration** pane, under the **Solution** node, select **Short Code**, right-click and select **New**.
3. In the right pane, in the **Code** box, type a CDN (Route Point) number. When this number is matched, the other short code fields activate. For example, type 3000, where 3000 is an Avaya Contact Center Select CDN (Route Point).
4. From the **Feature** list, select **Dial Extn**. If you do not see the **Dial Extn** option, ensure that you have selected the **Short Code** menu item under **Solution**, and not the local **Short Code** menu item for your IP Office. The Solution Short Code is common to all systems.
5. In the **Telephone Number** box, type the number output by the short code. For example, type the following: 6000|>>3000
 - Where 3000 is configured in Avaya Contact Center Select as a CDN (Route Point).
 - Where 6000 is the Avaya Contact Center Select SIP User Extension Number.

Note: Ensure there are no spaces in the **Telephone Number** box.

If a customer dials 3000, then 3000 is sent to telephone number 6000 and Avaya Contact Center Select.

6. Click **OK**.



Configuring Contact Recording

Before you begin

- Ensure the Media Manager application is installed, configured, and working on your IP Office.

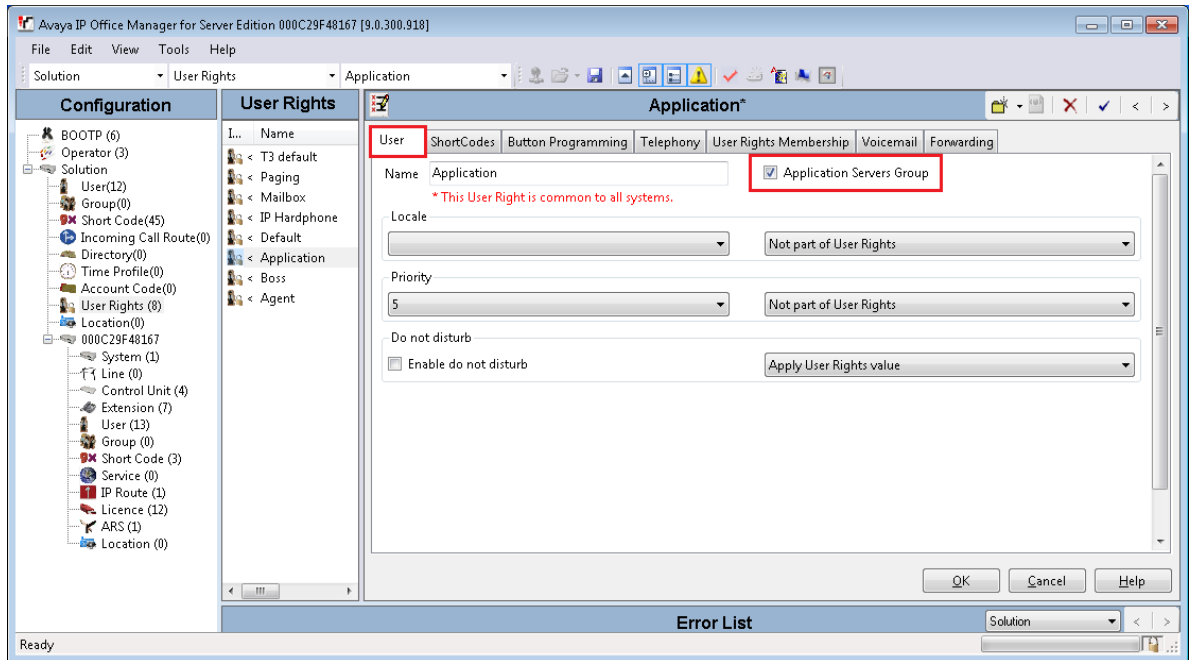
About this task

Configure the User and User Rights settings to enable Contact Recording for Avaya Contact Center Select agents and agent supervisors using IP Office.

Procedure

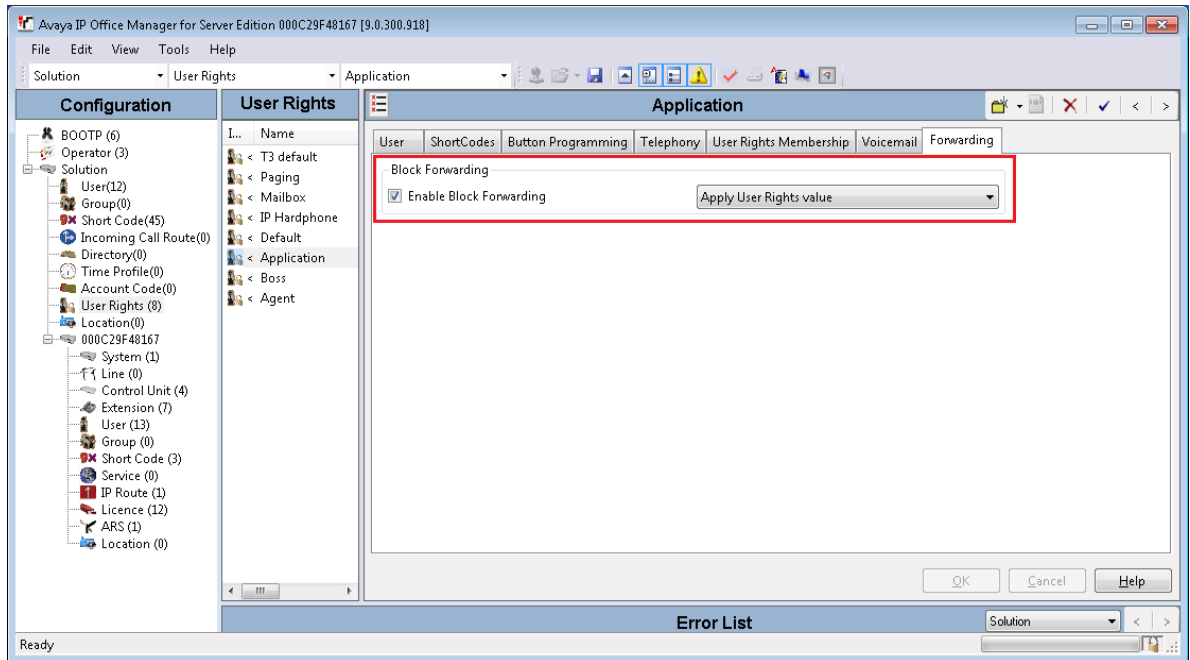
1. Using IP Office Manager, select the IP Office server in the **Configuration** pane.
2. In the **Configuration** pane, under the **Solution** node, select **User Rights**.
3. In the middle pane, select **Application**.
4. In the right **Application** pane, select the **User** tab.

5. Select Application Servers Group.



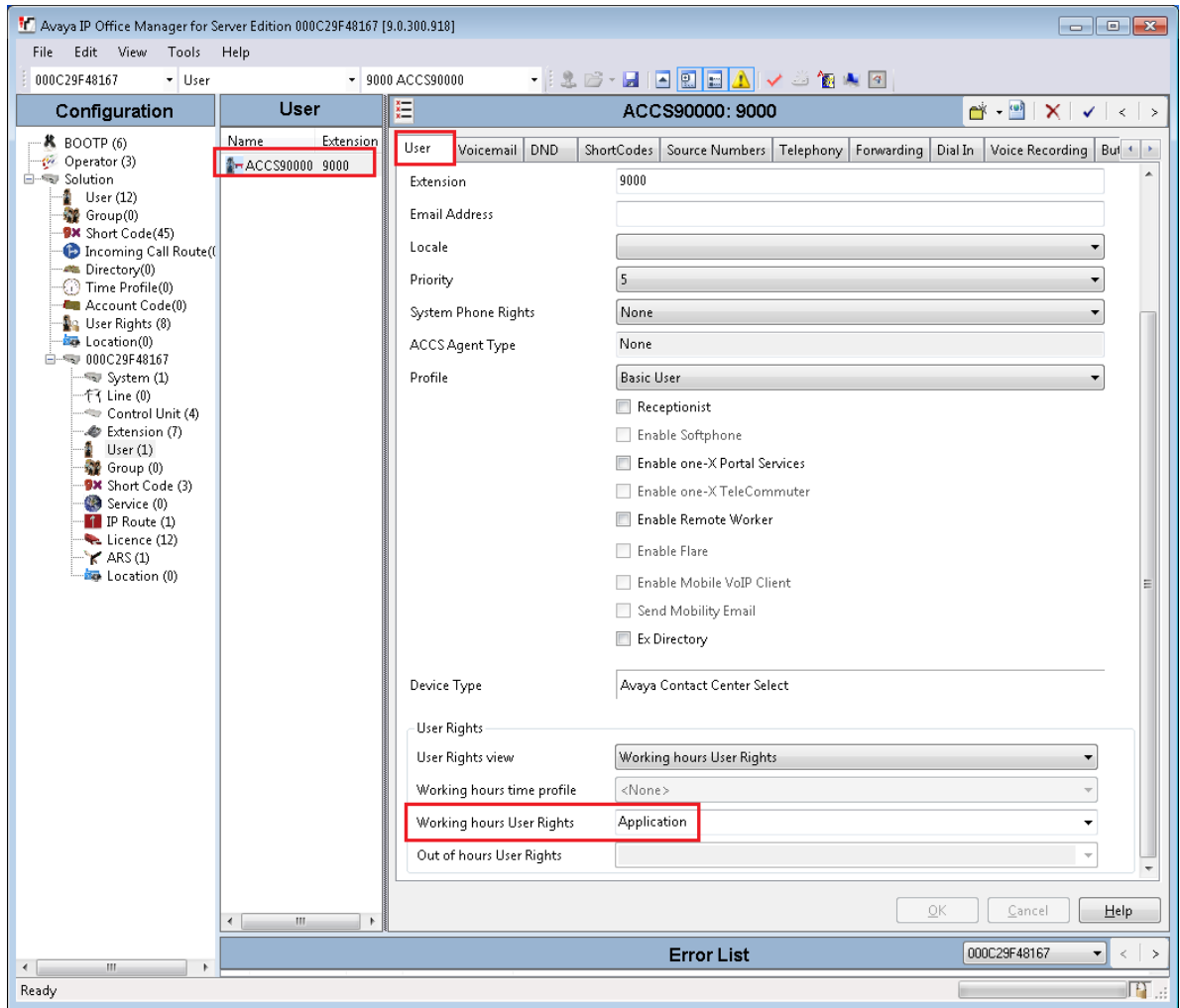
6. Click **OK**.
7. In the right **Application** pane, select the **Forwarding** tab.
8. Select **Enable Block Forward**.
9. From the list, select **Apply User Rights value**.

10. Click **OK**.



11. Using IP Office Manager, select the IP Office server in the **Configuration** pane.
12. In the **Configuration** pane, under the IP Office server, select **User**.
13. In the middle pane, select the Avaya Contact Center Select SIP User Extension.
14. In the right pane, select the **User** tab.
15. From the **Working hours Users Rights** list, select **Application**.

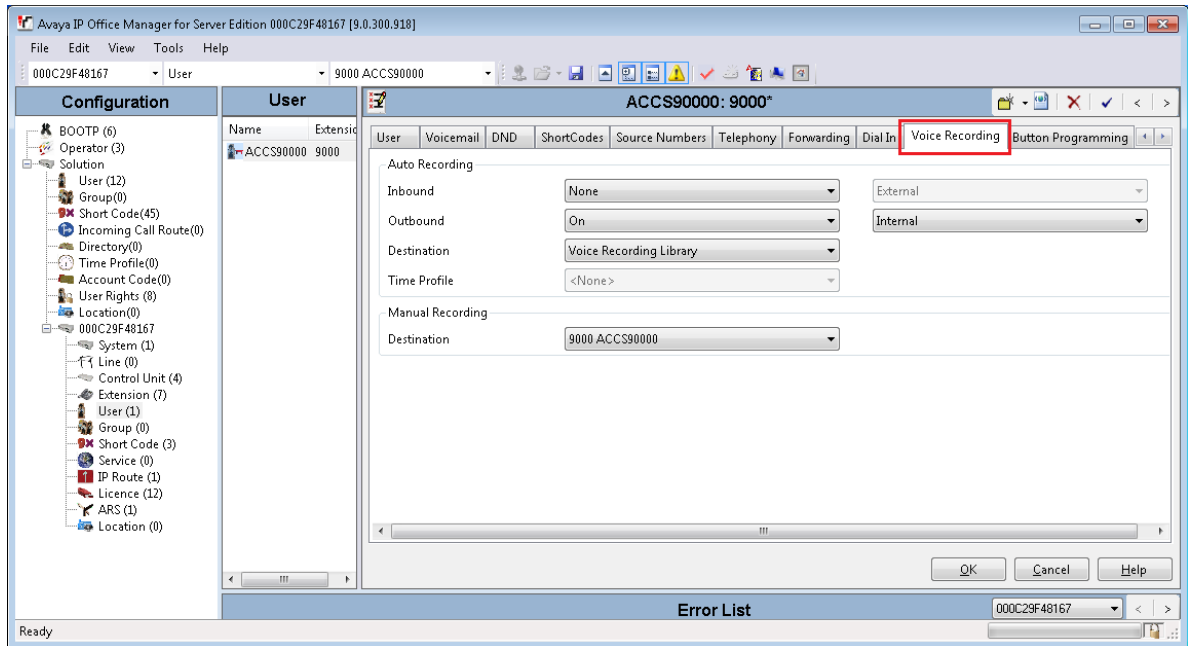
16. Click **OK**.



17. On the Avaya Contact Center Select SIP User Extension user, select the **Voice Recording** tab.

18. From the **Inbound** list, select **None**.

19. From the **Outbound** list, select **On**, and **Internal**.

20. From the **Destination** list, select **Voice Recording Library**.21. Click **OK**.

Configuring IP Office extensions

About this task

Use this procedure to configure an IP Office extension for Avaya Contact Center Select agents using SIP and H.323 physical desk phones.

! Important:

Use this procedure for desk phones only. Ignore this procedure if your Avaya Contact Center Select agents use Avaya Communicator or Avaya Workplace Attendant softphones for Windows with IP Office. Avaya Contact Center Select prevents creating an IP Office extension for an extension used by a softphone and prohibits using the same extension for a physical desk phone and a softphone.

When you create an agent in Avaya Contact Center Select, data synchronization ensures that a corresponding user is created in IP Office. For Avaya Contact Center Select agents using SIP and H.323 physical desk phones, IP Office must have an extension for every IP Office user. You can reuse existing IP Office extensions for this purpose. Alternatively, you must create one new IP Office extension for each IP Office user that corresponds to an Avaya Contact Center Select agent. Avaya Contact Center Select agents can then use these IP Office users and extensions to handle customer calls when they log on.

There are many different ways of providing a H.323 or SIP IP Office extension for each Avaya Contact Center Select agent, the following procedure describes one method. Some IP Office

Extension settings cannot be merged. Changes to these settings might require a reboot of the IP Office system.

! **Important:**

If your Avaya Contact Center Select agents are using Avaya Communicator for Windows with IP Office, do not create an extension for the corresponding IP Office users.

Procedure

1. Using IP Office Manager, select the IP Office server in the **Configuration** pane.
2. In the **Configuration** pane, under the IP Office server, select **Extension**.
3. Right-click and select **New > H323 Extension** or select **New > SIP Extension**.
4. On the **Extn** tab, in the **Extension Id** box, type an extension number.
The Extension ID is the physical ID of the extension port. IP Office Manager prepopulates the default value.
5. On the **Extn** tab, in the **Base Extension** box, type a base extension number.
The Base Extension is the extension number associated with the phone, that is the internal number you must dial to reach a user.
The Base Extension value must match the Extension value of a user. For more information, see [Configuring the SIP User Extension number](#) on page 42.
6. In the **Phone Password** box, type a password.
The password is only required for the H.323 extensions if you enable Media Security. For more information, refer to the IP Office documentation.
7. In the **Confirm Phone Password** box, retype the password.
8. Click **OK**.
9. Ensure the IP Office server has an extension, with a configured base extension number, for every IP Office user that corresponds to an Avaya Contact Center Select agent.

Saving the IP Office configuration data

Before you begin

- Install the IP Office Manager software on a client computer that can communicate with the IP Office server.

About this task

Use IP Office Manager to save your configuration changes to the IP Office server.

Procedure

1. In IP Office Manager, in the **Configuration** pane, select your IP Office server.

2. From the main IP Office Manager menu, select **File > Save Configuration**.
3. On the **Send Multiple Configurations** window, use the check box to select your IP Office server from the list.
4. Click **OK**.

IP Office Manager saves the offline configuration file to your IP Office server.

Part 2: Avaya Contact Center Select Software Appliance deployment

Deploy the Avaya Contact Center Select Software Appliance components in the following order:

1. [Avaya WebLM OVA deployment](#) on page 52
2. [Avaya Aura Media Server OVA deployment](#) on page 77
3. [Avaya Contact Center Select virtual machine deployment](#) on page 104

Chapter 7: Avaya WebLM OVA deployment

Deploy the Avaya WebLM OVA to provide solution licensing. You can deploy the Avaya WebLM OVA on the same VMware host server as the Contact Center virtual machine and the Avaya Aura® Media Server OVA. Alternatively, you can deploy the Avaya WebLM OVA standalone on a separate VMware host server.

For additional information about deploying the Avaya WebLM OVA, see *Avaya WebLM using VMware® in the Virtualized Environment Deployment Guide* available on the Avaya Support website at <http://support.avaya.com>.

After you have deployed WebLM, you can apply WebLM patches, feature packs, or service packs.

WebLM OVA

Contact Center supports the WebLM license manager server. For increased efficiency and flexibility, the WebLM license manager supports the VMware Virtual Appliance and Open Virtualization Archive (OVA) deployment mechanisms. In a virtualized Contact Center environment, you can use VMware to load the WebLM OVA package onto a separate virtual machine in your contact center solution. The virtualized Contact Center server can then use the virtualized WebLM server as the license manager.

The WebLM OVA contains a hardened Linux operating system.

The WebLM OVA requires the following:

vCPU	Minimum CPU speed	Virtual memory reservation	Number of NICs	Virtual disk storage reservation
1	2300 MHz	2 GB	1 shared	35 GB

*** Note:**

Do not change any of these WebLM OVA VMware virtual machine settings.

The WebLM OVA uses the following network mapping:

WebLM Server VM Interface	Application
Eth0	License management

The WebLM server for VMware is packaged as a vAppliance ready for deployment using either VMware vSphere Client or VMware vCenter.

Deploy the WebLM OVA using Disk Format - Thick Provision Lazy Zeroed. Avaya WebLM does not support thin provisioning in production environments.

WebLM OVA deployment procedures

About this task

This task flow shows you the sequence of procedures you perform to deploy the WebLM OVA.

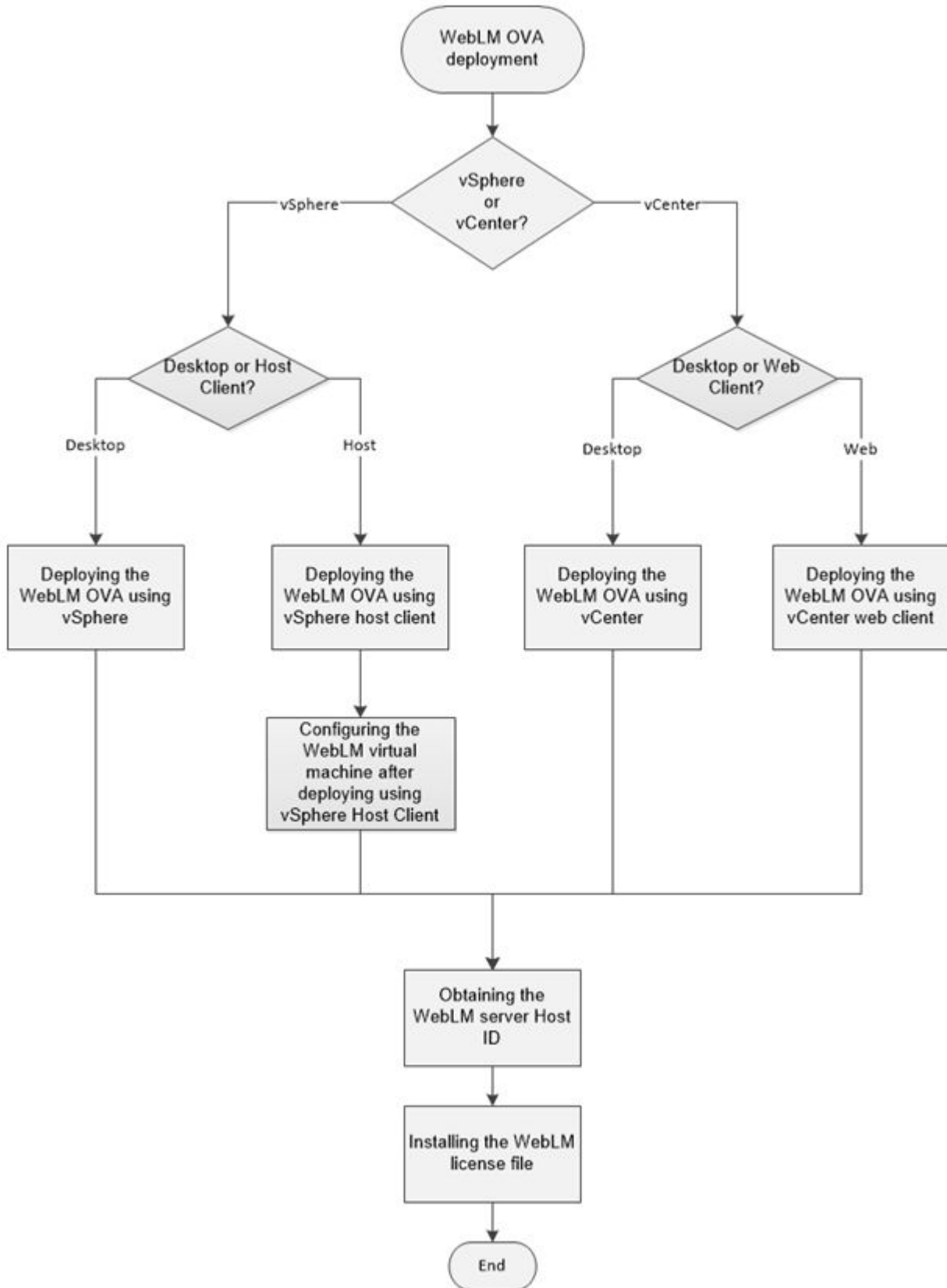


Figure 2: WebLM OVA deployment process

Deploying the WebLM OVA using vSphere (vSphere desktop client connected directly to ESXi host)

Before you begin

- Download the WebLM OVA file from the Avaya Product Licensing and Delivery System (PLDS) website at <https://plds.avaya.com/>.
- Know the IP address and network details of the WebLM server.

About this task

Deploy the WebLM OVA file onto a VMware ESXi host server. This creates a single instance of WebLM server for use in Contact Center solutions.

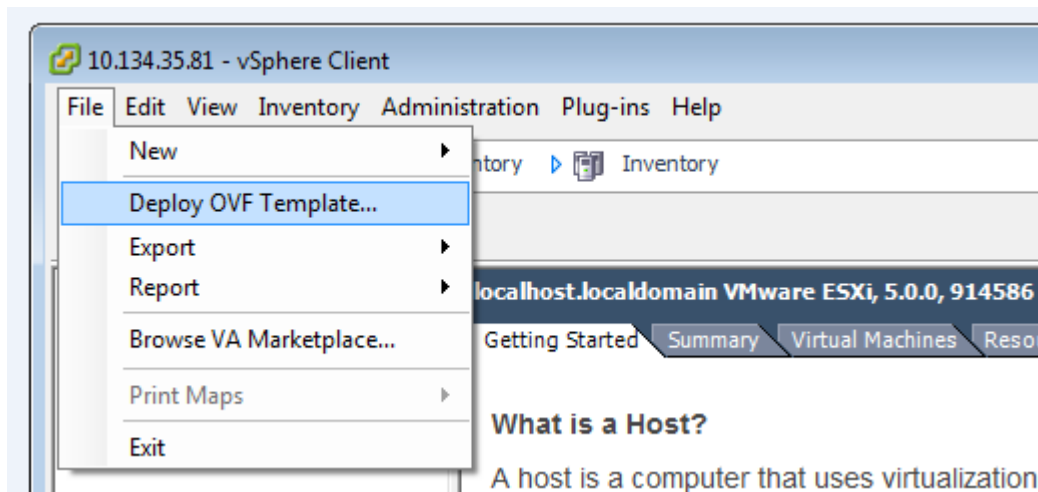
The WebLM OVA includes VMware tools. They are a suite of utilities that enhances the performance of the virtual machine's operating system and improves the management of the virtual machine.

Always deploy WebLM with a thick provisioned disk.

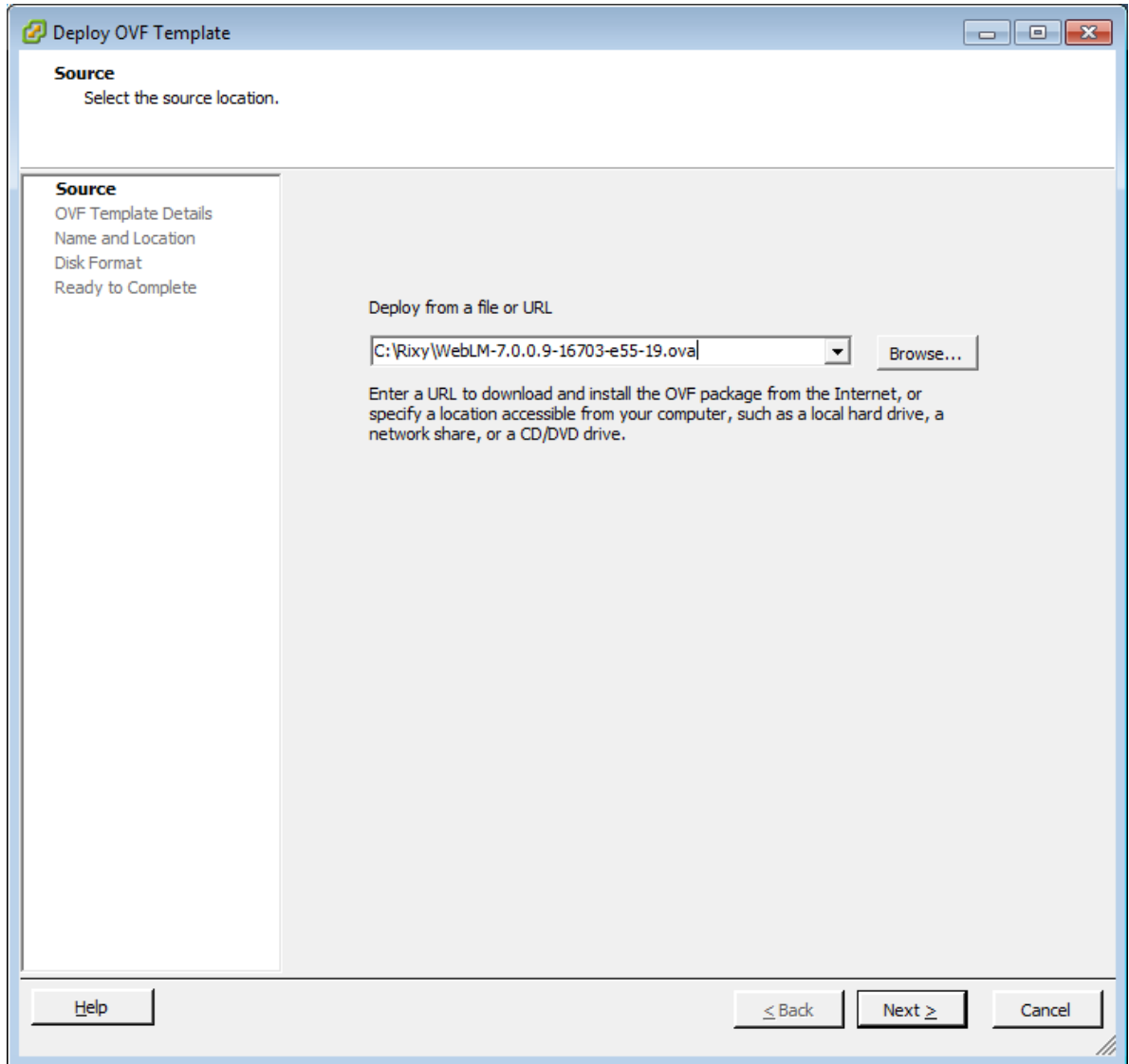
For best performance, use WebLM only on disks local to the ESXi Host, or SAN storage devices. Do not store WebLM on a NFS storage system.

Procedure

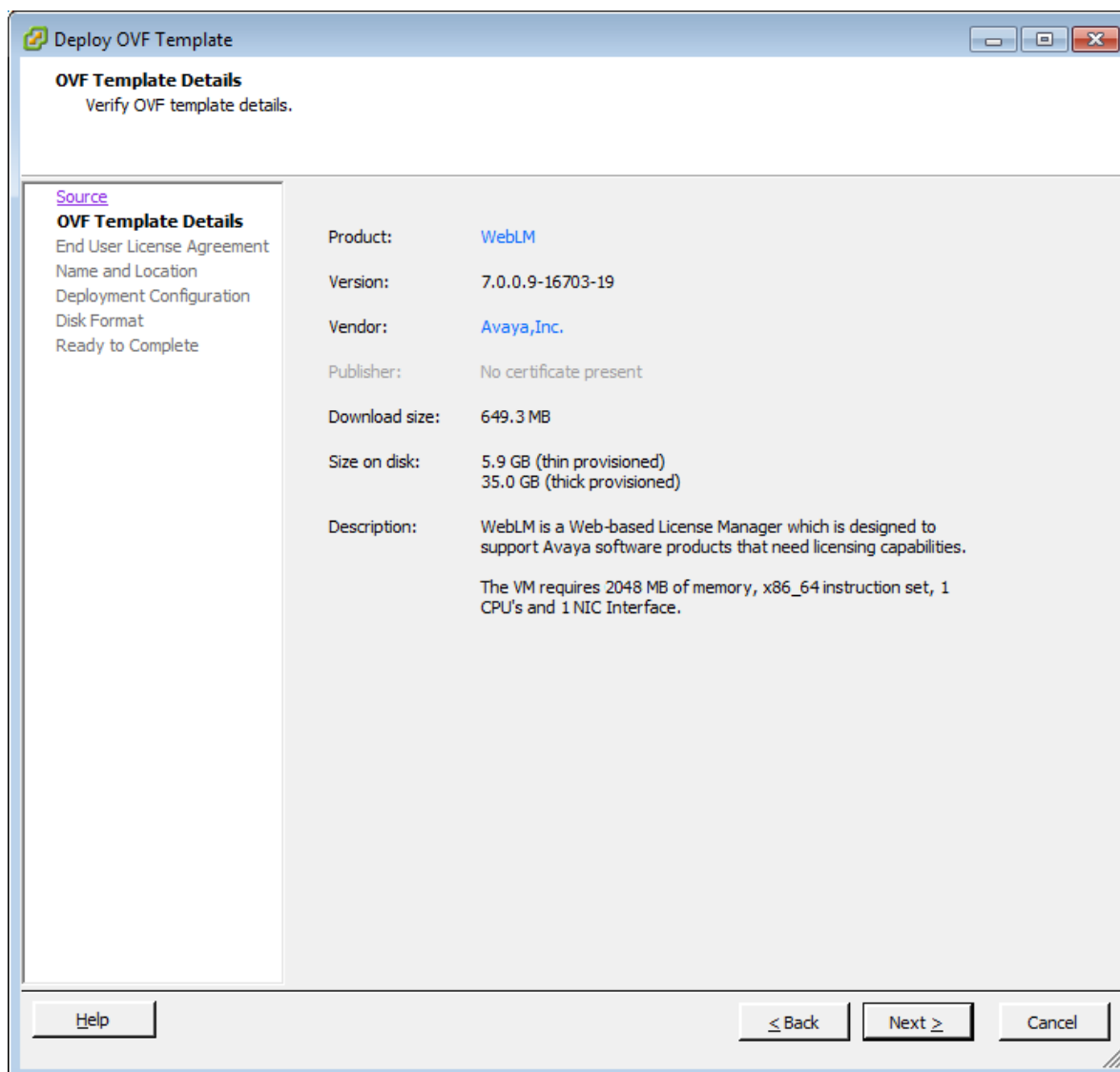
1. In your vSphere client, select the ESXi host server.
2. Select **File > Deploy OVF Template**.



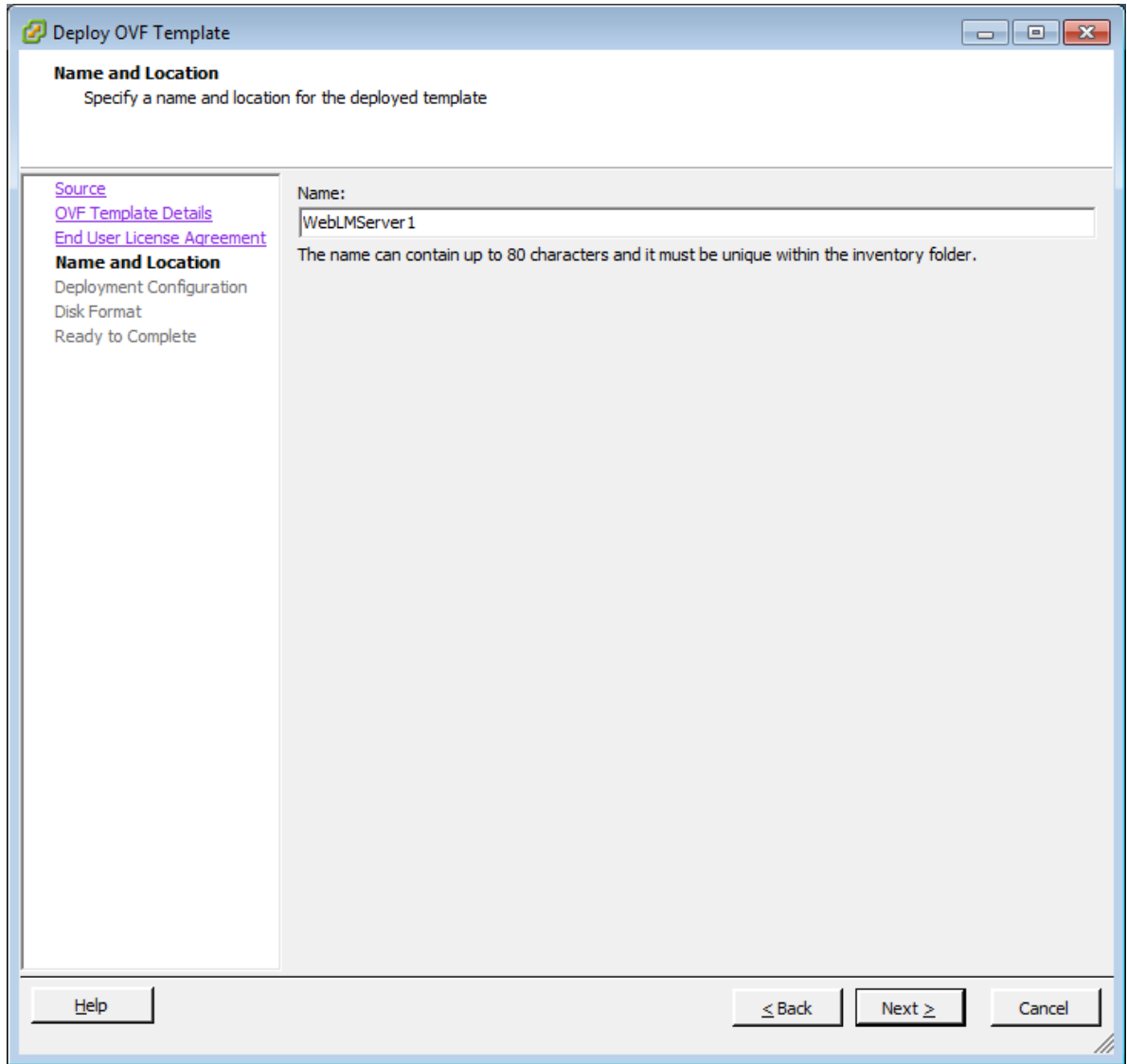
3. On the **Source** window, click **Browse**.
4. On the **Open** message box, select the WebLM OVA file.
5. Click **Open**.



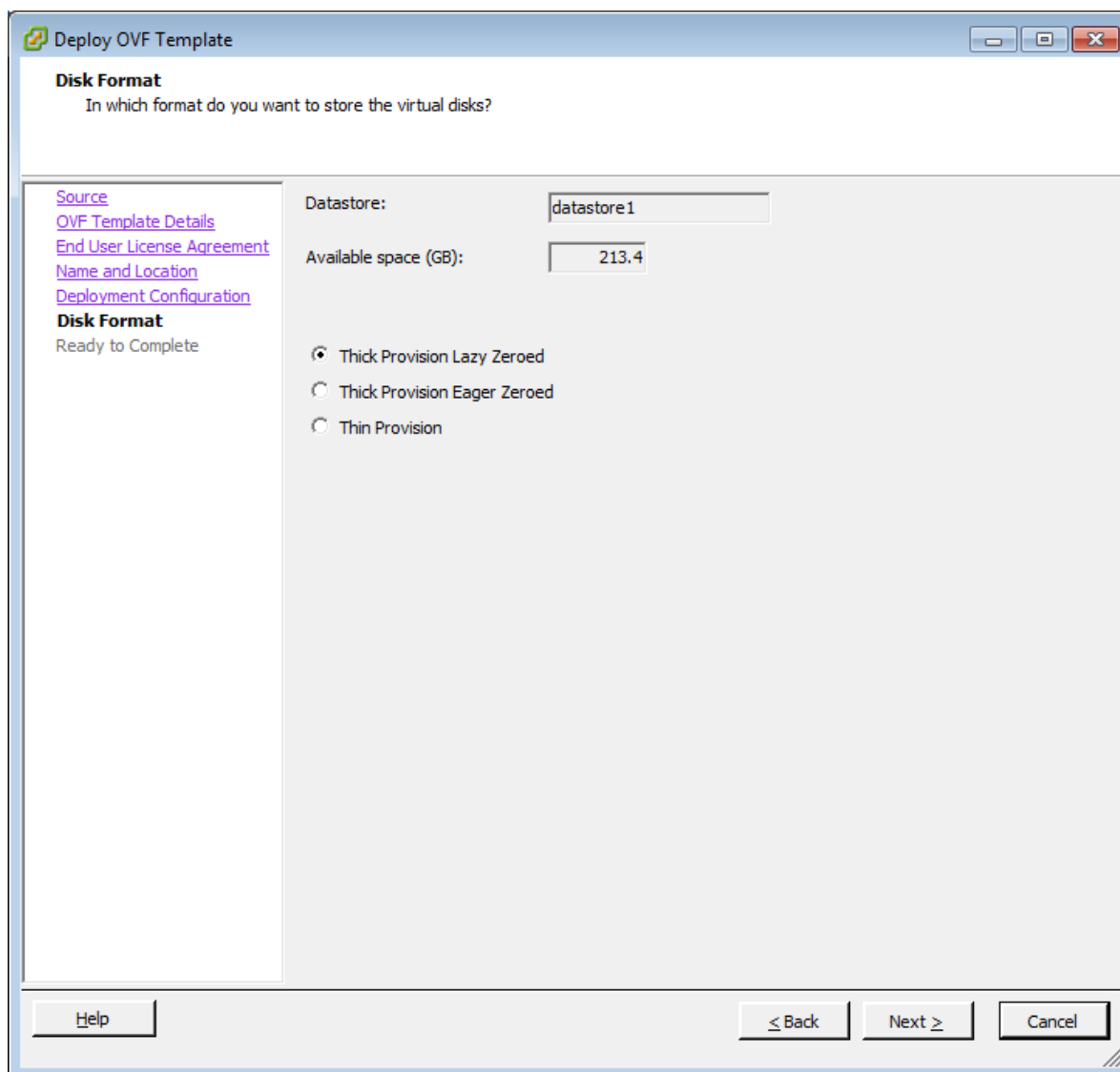
6. On the **Source** window, click **Next**.



7. On the **OVF Template Details** window, verify the details of the OVA template and click **Next**.
8. On the **End User License Agreement** window, read the license agreement, and if acceptable, click **Accept**.
9. Click **Next**.
10. On the **Name and Location** window, type the name of the new WebLM virtual machine. This is not the host name of the WebLM server. This is the name of the VMware virtual machine.



11. Click **Next**.
12. On the **Deployment Configuration** window, from the **Configuration** list, select **Profile –1**.
13. Click **Next**.
14. On the **Disk Format** window, select **Thick Provision Lazy Zeroed**.



15. Click **Next**.
16. On the **Ready to Complete** window, verify the deployment settings. If you need to modify any of the settings, click **Back**.
17. Click **Power on after deployment**.
18. Click **Finish**.
The WebLM template begins to load.
19. On the **Deployment Completed Successfully** message box, click **Close**.
20. In the vSphere client, from the inventory list in the left pane, select the new WebLM virtual machine.
21. With the deployed WebLM virtual machine still selected, right-click and select **Open Console**.

On the WebLM console screen, as the WebLM virtual machine boots, you are prompted to configure the network settings.

22. To configure the WebLM server network settings, enter `y` at the menu.
23. At the **IP Address** prompt, enter the IP address of the WebLM virtual machine. Use IPv4 formatting.
24. At the **Netmask** prompt, enter the subnet mask IP address. Use IPv4 formatting.
25. At the **hostname** prompt, enter the host name of the WebLM virtual machine.
26. At the **domain name** prompt, enter the name of the domain containing the WebLM virtual machine.
27. At the **default gateway** prompt, enter the Default Gateway IP address. Use IPv4 formatting.
28. At the **DNS server(s)** prompt, enter the DNS server IP address. Use IPv4 formatting.
29. At the **default Search List (optional)** prompt, enter a search list if you are using one.
30. At the **NTP Server IP or FQDN** prompt, enter the IP address or FQDN of your Network Time Protocol (NTP) server.
31. At the **Time Zone Detail** prompt, select the time zone continent or ocean for WebLM from the list.
32. At the **Please select a country** prompt, select the country for WebLM from the list.
33. Review the **Network Settings** and enter `y`.
The WebLM OVA deployment continues until the installation is complete.
34. With the WebLM virtual machine still selected, right-click and select **Open Console**.
WebLM provides a restricted shell to perform CLI based operations.

Deploying the WebLM OVA using vCenter (vSphere desktop client connected to vCenter)

Before you begin

- Download the WebLM OVA file from the Avaya Product Licensing and Delivery System (PLDS) website at <https://plds.avaya.com/>.
- Know the IP address and network details of the WebLM server.

About this task

Deploy the WebLM OVA file onto a VMware ESXi host server. This creates a single instance of WebLM server for use in Contact Center solutions.

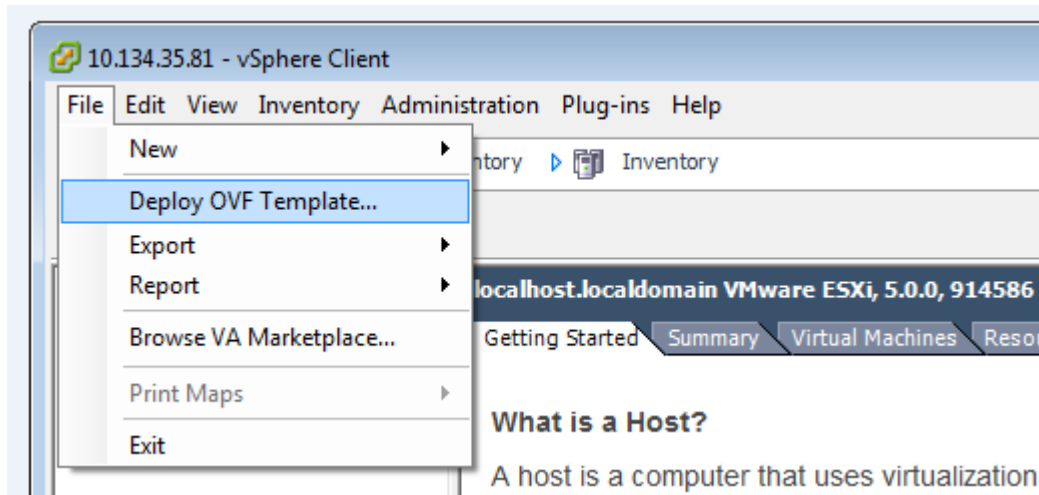
The WebLM OVA includes VMware tools. They are a suite of utilities that enhances the performance of the virtual machine's operating system and improves the management of the virtual machine.

Always deploy WebLM with a thick provisioned disk.

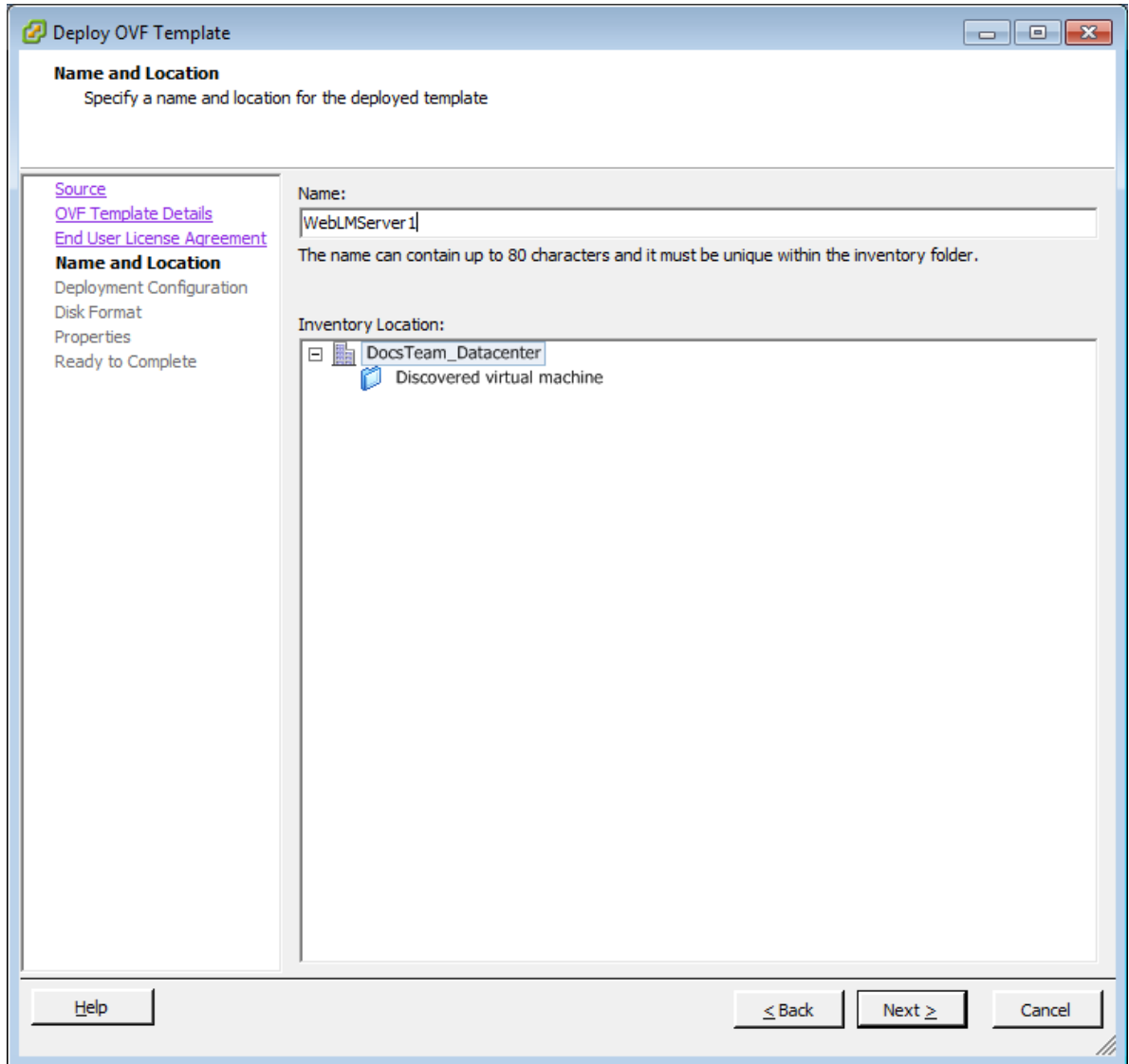
For best performance, use WebLM only on disks local to the ESXi Host, or SAN storage devices. Do not store WebLM on a NFS storage system.

Procedure

1. In your vSphere client, select **File > Deploy OVF Template**.



2. On the **Source** window, click **Browse**.
3. On the **Open** message box, select the WebLM OVA file.
4. Click **Open**.
5. On the **Source** window, click **Next**.
6. On the **OVF Template Details** window, verify the details of the OVA template and click **Next**.
7. On the **End User License Agreement** window, read the license agreement, and if acceptable, click **Accept**.
8. Click **Next**.
9. On the **Name and Location** window, in the **Name** box, type the name of the new WebLM virtual machine. This is not the host name, this is the name of the VMware virtual machine.



10. Click **Next**.
11. On the **Deployment Configuration** window, from the **Configuration** list, select **Profile –1**.
12. Click **Next**.
13. On the **Host and Cluster** window, select the host server or cluster on which to deploy the WebLM OVA. If you selected a cluster, select a **Specific Host** on that cluster.
14. Click **Next** to display the **Storage** window.
15. From the **Select a destination storage for the virtual machine files** list, select a location to store the WebLM virtual machine image.
16. Click **Next**.
17. On the **Disk Format** window, select **Thick Provision Lazy Zeroed**. Thin provisioning is not supported in production environments.

18. Click **Next**.

The screenshot shows the 'Deploy OVF Template' window with the 'Properties' section selected. The 'Application' section contains the following fields and error messages:

- Please enter the IP Address to assign to the VM:** [Empty field]
 Enter an IP address.
- Please enter the Netmask to assign to the VM:** [255 , 255 , 255 , 0]
 (Note: The netmask is already filled with a placeholder value)
- Please enter the IP Address of your default gateway:** [Empty field]
 Enter an IP address.
- Please enter the IP Address of your DNS server: [Multiple IP's separated by comma]**
 [Empty field]
 A value must be provided.
- Please enter the Short Hostname to assign to the VM:**
 [Empty field]
 A value must be provided.

At the bottom of the 'Application' section, a red error message states: "Properties with invalid values will be left unassigned. The vApp will not be able to power on until all properties have valid values."

The 'Properties' section on the left is marked as 'Ready to Complete'. The bottom of the window has buttons for 'Help', '≤ Back', 'Next ≥', and 'Cancel'.

19. On the **Network Mapping** window, configure a network interface for the WebLM virtual machine.
20. Click **Next**.
21. In the **Properties** window, in the **Please enter the IP Address to assign to the VM** box, type the IP address of the WebLM virtual machine. Use IPv4 formatting.
22. In the **Please enter the Netmask to assign to the VM** box, type the subnet mask IP address. Use IPv4 formatting.
23. In the **Please enter the IP Address of your default Gateway** box, type the Default Gateway IP address. Use IPv4 formatting.

24. In the **Please enter the IP Address of your DNS server** box, type the DNS server IP address. Use IPv4 formatting.
25. In the **Please enter the Short Hostname to assign to the VM** box, type the short hostname of the WebLM server.
26. In the **Please enter the Domain Name to assign to the VM** box, type the domain name of the WebLM server.
27. From the **Please select the Time Zone** list, select the time zone for the solution.
28. Click **Next**.
29. On the **Ready to Complete** window, verify the deployment settings. If you need to modify any of the settings, click **Back**.
30. Click **Power on after deployment**.
31. Click **Finish**.
The WebLM template begins to load.
32. On the **Deployment Completed Successfully** message box, click **Close**.

Deploying the WebLM OVA using vSphere host client

Before you begin

- Download the WebLM OVA file from the Avaya Product Licensing and Delivery System (PLDS) website at <https://plds.avaya.com/>.
- Know the IP address and network details of the WebLM server.

About this task

Deploy the WebLM OVA file onto a VMware ESXi host server. This creates a single instance of WebLM server for use in Contact Center solutions.

The WebLM OVA includes VMware tools. They are a suite of utilities that enhances the performance of the virtual machine's operating system and improves the management of the virtual machine.

Always deploy WebLM with a thick provisioned disk.

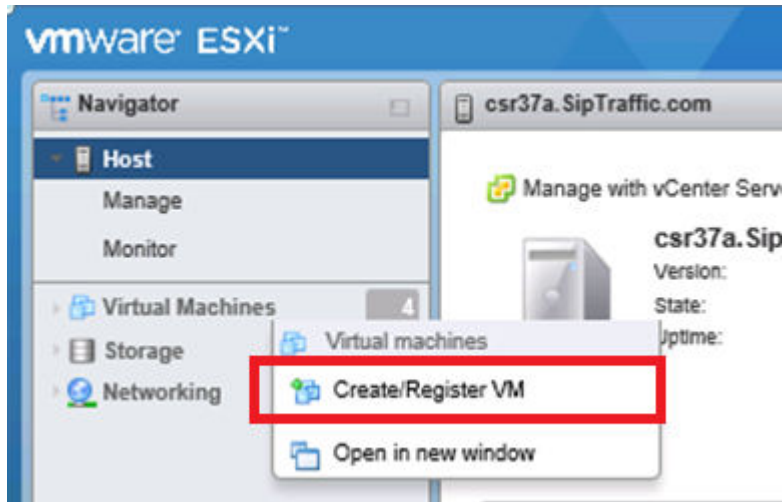
For best performance, use WebLM only on disks local to the ESXi Host, or SAN storage devices. Do not store WebLM on a NFS storage system.

Note:

The vSphere host client is a HTML5 client.

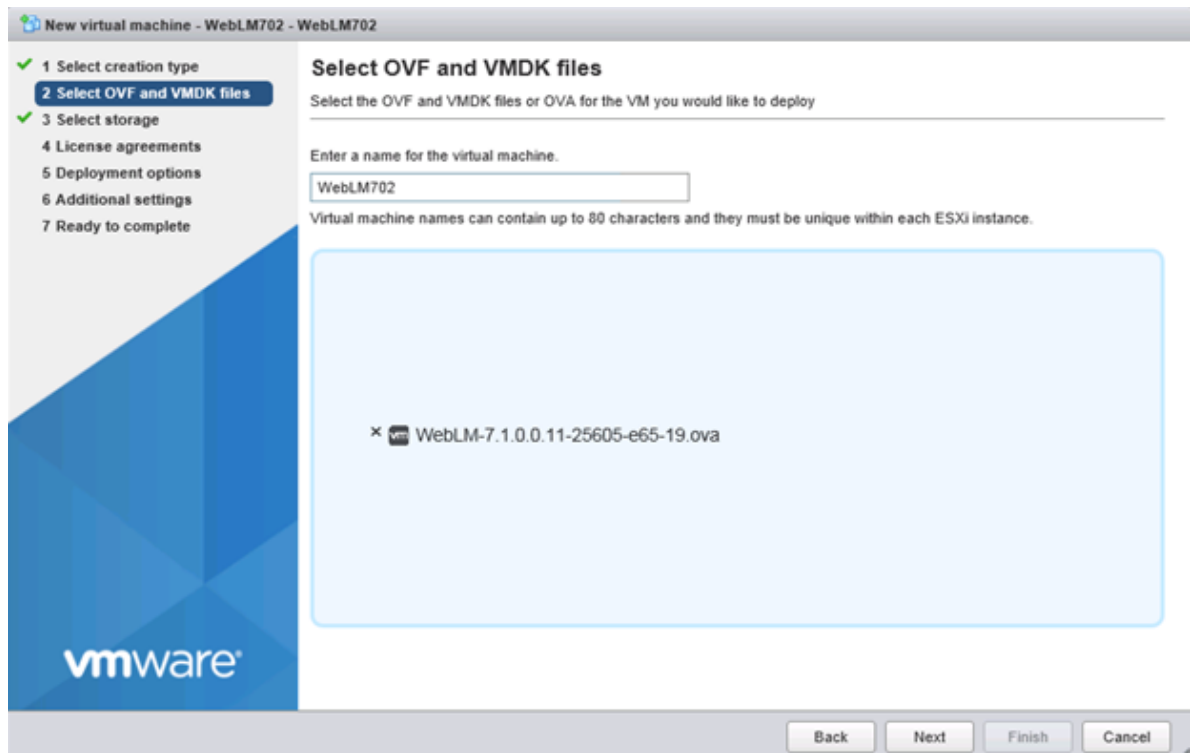
Procedure

1. In your vSphere host client, right-click on **Virtual Machines** and select **Create/Register VM**.



2. Under **Select creation type**, select **Deploy a virtual machine from an OVF or OVA file**.
3. Click **Next**.
4. Under **Select OVF and VMDK files**, type a name for the virtual machine.
5. Click **Browse** and select the WebLM OVA file.

6. Click **Next**.



7. Under **Select storage**, select a datastore location to store the WebLM virtual machine image. Ensure that the storage location you select has sufficient available storage space to store a thick provisioned virtual machine image.
8. Click **Next**.
9. Under **License agreements**, read the End User License Agreement and click **I agree**.
10. Click **Next**.
11. Under **Deployment options**, select the **Network mappings** and under Disk provisioning select **Thick**.
12. Click **Next**.
13. On the **Additional settings** page, under **Application**, in the **Please enter the IPv4 Address to assign to the VM** box type the IP address of the WebLM server.
14. In the **Please enter the Netmask to assign to the VM** box, type the subnet mask IP address.
15. In the **Please enter the IPv4 Address of your default gateway** box, type the default gateway IP address.
16. In the **Please enter the IP Address of your DNS server** box, type the IP address of one or more DNS servers. Use IPv4 formatting. Separate the IP addresses with a comma.
17. In the **Please enter the Short Hostname to assign to the VM** box, type the name of the WebLM server.

18. In the **Please enter the Domain Name to assign to the VM** box, type the domain name for the WebLM server.
19. In the **Please provide NTP Server IP/FQDN** box, type a comma separated list of NTP servers. You use the NTP server to synchronize servers with each other and with the contact center solution.
20. In the **Please select the Time Zone** box, enter the Timezone for the WebLM server.
21. Under **WebLM CLI USER**, in the **Please enter the WebLM command line user name** box, type the name for the command line user.
22. In the **Please enter the WebLM command line user password** box, type the password for the command line user. Confirm the password.
23. Under **WebLM UI Password for User – admin**, in the **Please enter the WebLM UI admin user password** box, type the password for the WebLM UI admin user. Confirm the password.

New virtual machine - WebLM702 - WebLM702

1 Select creation type
 2 Select OVF and VMDK files
 3 Select storage
 4 License agreements
 5 Deployment options
 6 Additional settings
 7 Ready to complete

Additional settings

Additional properties for the VM

Application	
Please enter the IPv4 Address to assign to the VM:	<input type="text" value="172.18.69.235"/>
Please enter the Netmask to assign to the VM:	<input type="text" value="255.255.248.0"/>
Please enter the IPv4 Address of your default gateway:	<input type="text" value="172.18.71.254"/>
Please enter the IP Address of your DNS server: [Multiple IP's separated by comma]	<input type="text" value="172.18.71.252"/>
Please enter the Short Hostname to assign to the VM:	<input type="text" value="WebLM702"/>
IPv6 Address. Please enter IPv6 address (optional) :	<input type="text"/>
IPv6 Network Prefix. Please enter IPv6 Network Prefix (Optional) :	<input type="text" value="64"/>
IPv6 Gateway. Please enter IPv6 Gateway (optional) :	<input type="text"/>
Please enter the Domain Name	<input type="text" value="siptraffic.com"/>

Back Next Finish Cancel

24. Click **Next**.
25. Under **Ready to complete**, review and verify the deployment settings. If you need to modify any of the settings, click **Back**.
26. Click **Finish**.

 **Important:**

Do not refresh your browser while the VM is being deployed.

Next steps

When the WebLM OVA has been successfully deployed the virtual machine will be powered on automatically. If the virtual machine is not powered on automatically, power on the WebLM virtual machine.

After deploying the WebLM OVA using the vSphere host client, you might need to re-enter the configuration data after starting the WebLM virtual machine for the first time. If WebLM prompts you to configure the appliance after you start the virtual machine, then you must re-enter the configuration data. See [Configuring the WebLM virtual machine after deploying using the vSphere Host Client](#) on page 72.

Deploying the WebLM OVA using vSphere web client

Before you begin

- Download the WebLM OVA file from the Avaya Product Licensing and Delivery System (PLDS) website at <https://plds.avaya.com/>.
- Know the IP address and network details of the WebLM server.

About this task

Deploy the WebLM OVA file onto a VMware ESXi host server. This creates a single instance of WebLM server for use in Contact Center solutions.

The WebLM OVA includes VMware tools. They are a suite of utilities that enhances the performance of the virtual machine's operating system and improves the management of the virtual machine.

Always deploy WebLM with a thick provisioned disk.

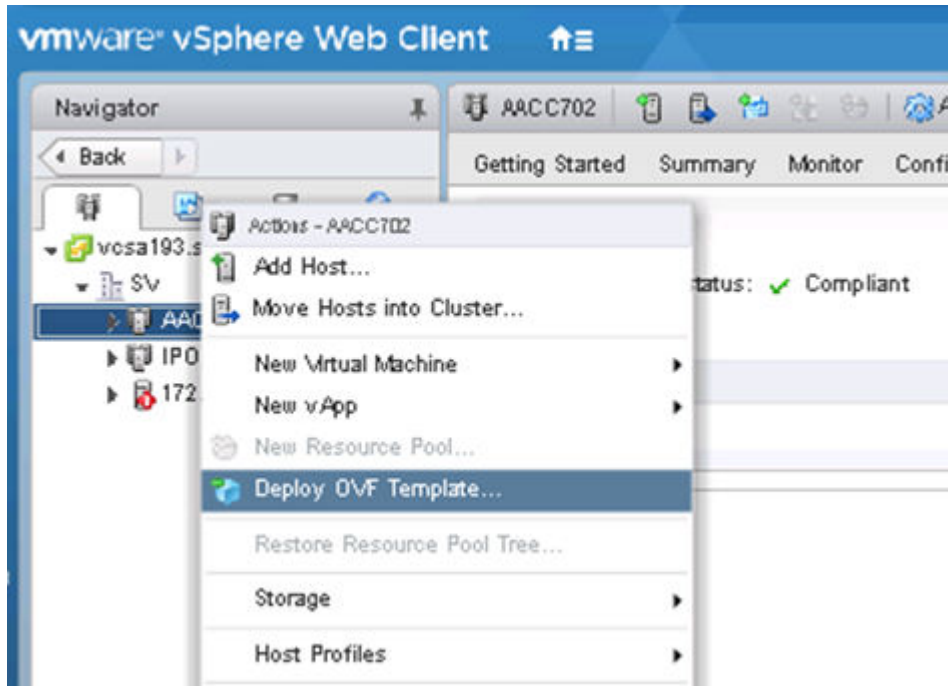
For best performance, use WebLM only on disks local to the ESXi Host, or SAN storage devices. Do not store WebLM on a NFS storage system.

 **Note:**

The vSphere web client is supported with vCenter deployments only.

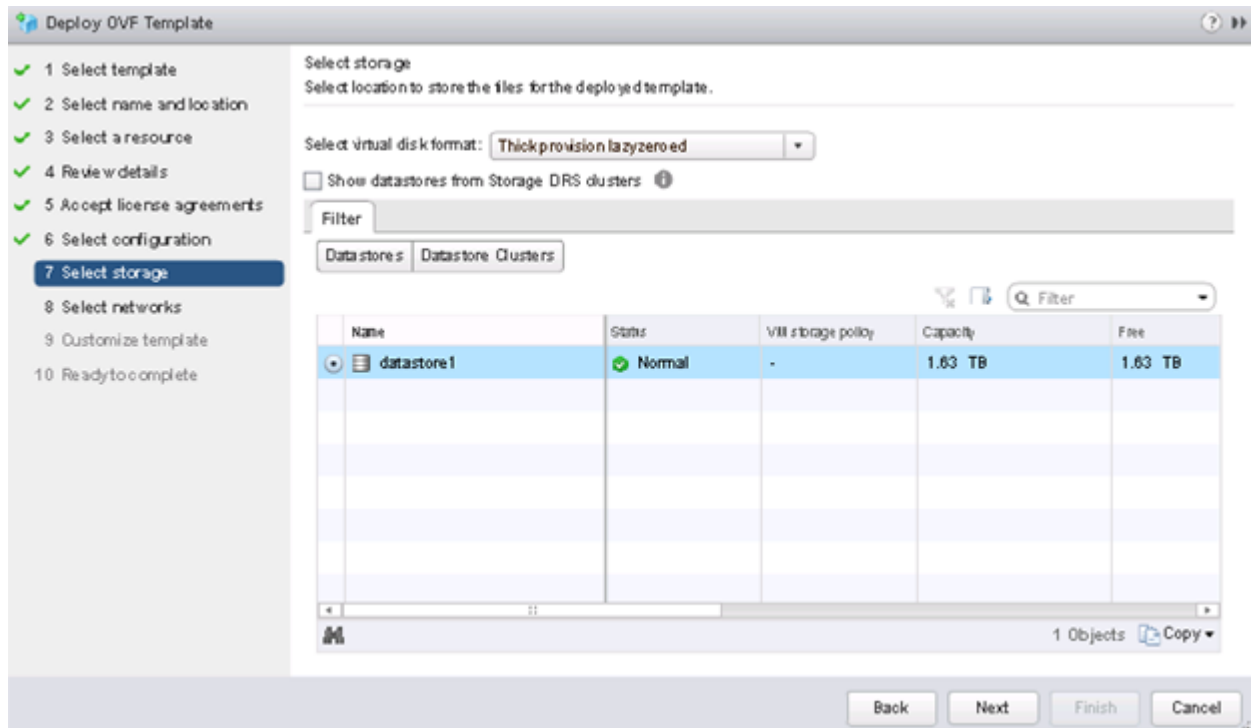
Procedure

1. In your vSphere web client, right-click in the **Navigator pane** and select **Deploy OVF Template**.



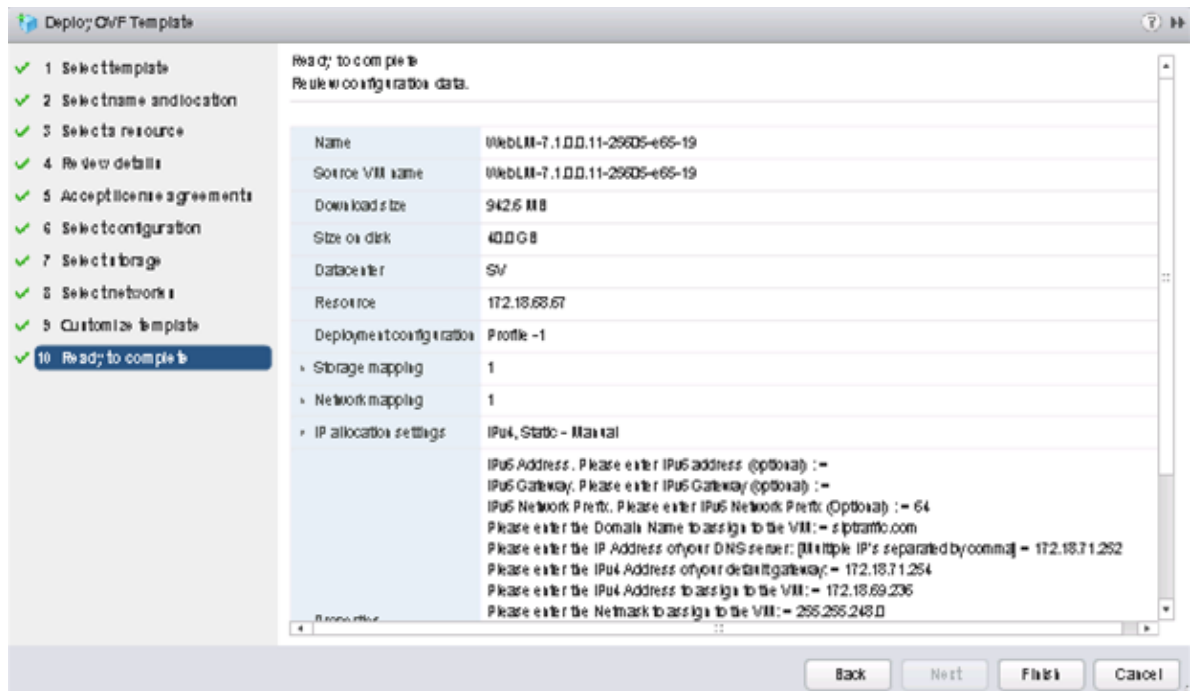
2. On the **Select template** page, select **Local file** and click **Browse** to select the WebLM OVA file.
3. Click **Next**.
4. On the **Select name and location** page, in the **Name** box, type a name for the virtual machine.
5. Select a datacenter location for the WebLM virtual machine.
6. Click **Next**.
7. On the **Select a resource** page, navigate to and select the host where you want to deploy the WebLM virtual machine.
8. Click **Next**.
9. On the **Review details** page, review the WebLM details.
10. Click **Next**.
11. On the **Accept license agreements** page, read the license agreement and click **Accept**.
12. Click **Next**.
13. On the **Select configuration** page, accept the default profile 1.
14. Click **Next**.

15. On the **Select storage** page, from the **Select virtual disk format** drop-down list, select **Thick provision lazy zeroed**.
16. Select a location to store the WebLM virtual machine image. Ensure that the storage location you select has sufficient available storage space to store a thick provisioned virtual machine image.



17. Click **Next**.
18. On the **Select networks** page, select the destination network for the WebLM virtual machine from the drop-down list.
19. Click **Next**.
20. On the **Customize template** page, under **Application**, in the **Please enter the Domain Name to assign to the VM** box type the domain name for the WebLM server.
21. In the **Please enter the IP Address of your DNS server** box, type the IP address of one or more DNS servers. Use IPv4 formatting. Separate the IP addresses with a comma.
22. In the **Please enter the IPv4 Address of your default gateway** box, type the default gateway IP address.
23. In the **Please enter the IPv4 Address to assign to the VM** box, type the IP address of the WebLM server.
24. In the **Please enter the Netmask to assign to the VM** box, type the subnet mask IP address.
25. In the **Please enter the Short Hostname to assign to the VM** box, type the name of the WebLM server.

26. In the **Please provide NTP Server IP/FQDN** box, type a comma separated list of NTP servers. You use the NTP server to synchronize servers with each other and with the contact center solution.
27. In the **Please select the Time Zone** box, enter the Timezone for the WebLM server.
28. Under **Enhanced Access Security Gateway(EASG)**, in the **EASG User Access** box, type 1 to enable EASG or type 2 to disable EASG.
29. Under **WebLM CLI USER**, in the **Please enter the WebLM command line user name** box, type the name for the command line user.
30. In the **Please enter the WebLM command line user password** box, type the password for the command line user. Confirm the password.
31. Under **WebLM UI Password for User – admin**, in the **Please enter the WebLM UI admin user password** box, type the password for the WebLM UI admin user. Confirm the password.
32. Click **Next**.
33. Under **Ready to complete**, review and verify the deployment settings. If you need to modify any of the settings, click **Back**.



34. Click **Finish**.

! **Important:**

Do not refresh your browser while the VM is being deployed.

Next steps

When the WebLM OVA has been successfully deployed, power on the virtual machine.

Configuring the WebLM virtual machine after deploying using the vSphere Host Client

About this task

After you power on the WebLM virtual machine for the first time, enter the WebLM configuration data.

Procedure

1. Connect to the WebLM virtual machine, using the VMware console, after you power on the virtual machine for the first time.
2. When the **Provide user input configuration** prompt appears, type **Y** and press **Enter**.
3. At the **Please enter the IP Address to assign to the VM** prompt type the IP address of the WebLM server and press Enter.
4. At the **Please enter the Netmask to assign to the VM** prompt, type the subnet mask IP address and press Enter.
5. At the **Please enter the IPv4 Address of your default gateway** prompt, type the default gateway IP address and press Enter.
6. At the **Please enter the Short Hostname to assign to the VM** prompt, type the name of the WebLM server and press Enter.
7. At the **Please enter the Domain Name to assign to the VM** prompt, type the domain name for the WebLM server and press Enter.
8. At the **Please enter the IP Address of your DNS server** box, type the IP address of one or more DNS servers and press Enter. Use IPv4 formatting. Separate the IP addresses with a comma.
9. At the **Please enter the Management IPV6 Address to assign to the VM** prompt, press Enter to skip.
10. At the **Please Enter the default Search List** prompt, press Enter to skip.
11. At the **Please provide NTP Server IP/FQDN** prompt, type a comma separated list of NTP servers and press Enter. You use the NTP server to synchronize servers with each other and with the contact center solution.
12. At the **WebLM CLI User Name** prompt, type the name for the command line user and press Enter. Note the provided list of WebLM CLI user names that you must not use.
13. At the **WebLM CLI User Password** prompt, type the password for the command line user and press Enter. Confirm the password.

14. At the **WebLM UI Admin User Password** prompt, type the password for the WebLM UI admin user and press Enter. Confirm the password.
15. At the **WebLM CLI User Password** prompt, type the password for the command line user and press Enter. Confirm the password.
16. At the **Enter 1 to Enable EASG (Recommended) or 2 to Disable EASG** prompt, enter 1 to enable EASG or 2 to disable EASG and press Enter.
17. At the **Please select a continent or ocean** prompt, type the number that relates to your continent or ocean and press Enter.
18. At the **Please select a country** prompt, type the number that relates to your country and press Enter.
19. At the **Please select one of the following time zone regions** prompt, type the number that relates to your time zone region and press Enter.
20. Review the Network Settings and press Enter.
21. Review WebLM CLI User, WebLM UI admin User, and EASG settings, type `y` to continue or type `n` to go back and make changes to the configuration data. Press Enter and wait for the WebLM server to apply the configuration data.
22. Close the console session.
23. Restart the WebLM virtual machine.

Obtaining the WebLM server Host ID

Before you begin

- Deploy the WebLM OVA on your VMware host server.

About this task

Obtain the WebLM server Host ID so you can use it to obtain or generate a license for use by Contact Center features.

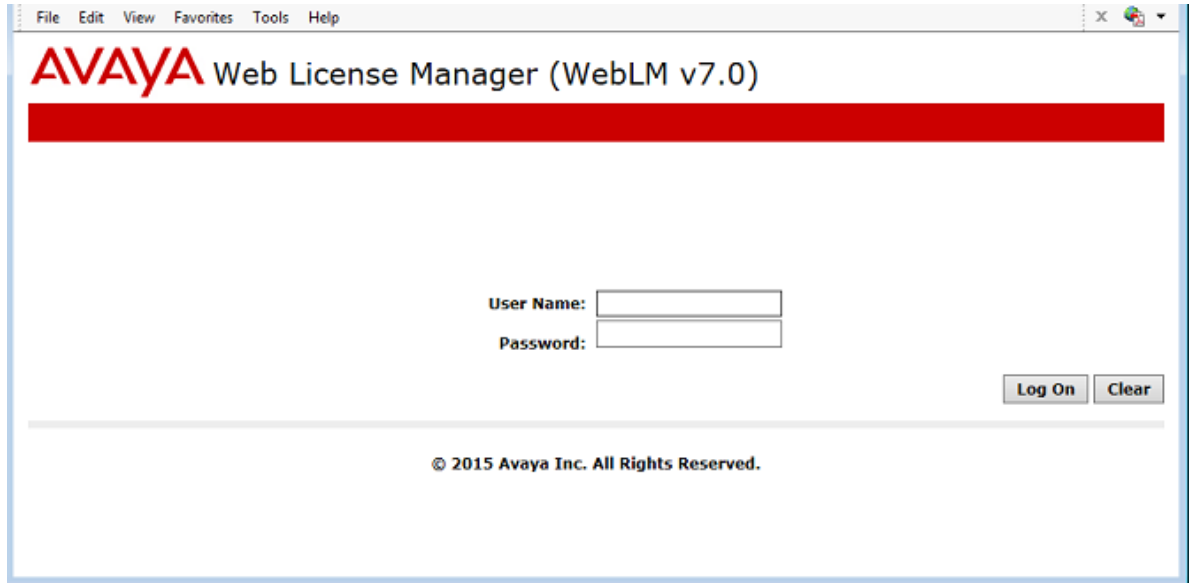
The first time you log in to the WebLM Web interface, you must change the default password.

Procedure

1. Open Internet Explorer and enter the following URL:

`https://<WebLMIPAddress>:52233/WebLM/index.jsp`

Where WebLMIPAddress is the IP address of the WebLM virtual machine.



2. Log in to the Web License Manager user interface using the default settings:
The default **User Name** is admin.
The default **Password** is weblmadmin.
3. Click **Log On**.
4. You are forced to change the password and log back on again using the new password.
5. On the left hand pane, select **Server properties**.



6. Record the Server Host ID **Primary Host ID** number.
7. Use the WebLM server Host ID to obtain Contact Center licenses from the Avaya Product Licensing and Delivery System (PLDS).

Installing the WebLM license file

Before you begin

- Use the WebLM server Host ID to obtain Contact Center licenses from the Avaya Product Licensing and Delivery System (PLDS).

About this task

Install the WebLM license file to license Contact Center features and agents.

Procedure

1. Open Internet Explorer and enter the following URL:

`https://<WebLMIPAddress>:52233/WebLM/index.jsp`

Where WebLMIPAddress is the IP address of the WebLM virtual machine.

2. Log in to the Web License Manager user interface using the “admin” **User Name** and your new password.
3. Log in to the WebLM Web interface using your new password.
4. In the left hand pane, click **Install license**.
5. In the **Enter license path** box, enter the license file details. Alternatively, click **Browse** to load the license file.
6. Click **Install**.
7. You can review the Contact Center licensed details by clicking **Licensed products > CCTR > ContactCenter**.

AVAYA Web License Manager (WebLM v7.0) Help | About | Change Password | Log off admin

- WebLM Home
- Install license
- Licensed products
- CCTR
- ▼ ContactCenter
 - View license capacity
 - View peak usage
- Uninstall license
- Server properties
- Manage users
- Shortcuts
- Help for Installed Product

Contact Center - Release: 7 - SID: 101030
Standard License file

You are here: Licensed Products > ContactCenter > View License Capacity

License installed on: September 9, 2015 1:22:07 PM +01:00

License File Host IDs: VF-39-FF-06-31-06

Licensed Features

30 Items Show 15 ▼

Feature (License Keyword)	Expiration date	Licensed capacity	Currently Used
Maximum AMS Instance VALUE_CCTR_AMS_INSTANCE	permanent	1	0
Base Offer VALUE_CCTR_BASE	permanent	ENTERPRISE	Not counted
Maximum Contact Center Manager Standard Nodes VALUE_CCTR_CCM_STD_NODE	permanent	1	0
Maximum Open Interface VALUE_CCTR_OI	permanent	2000	0
Maximum License Managers VALUE_CCTR_PLICD	permanent	1	0
Maximum Basic Port VALUE_CCTR_BASIC_PORT	permanent	2000	0
Maximum SMS Agents VALUE_CCTR_SMS_AGENT	permanent	2000	0

WebLM licensing is now available for Contact Center.

Chapter 8: Avaya Aura[®] Media Server OVA deployment

Deploy the Avaya Aura[®] Media Server OVA to provide the media services required by SIP-enabled Contact Center.

The Avaya Aura[®] Media Server OVA creates and configures a virtual machine containing Avaya Aura[®] Media Server software. The resulting virtual machine contains a Linux operating system, hard disk drive, third-party components, system configuration, firewall settings, and Avaya Aura[®] Media Server application software.

You can deploy the Avaya Aura[®] Media Server OVA on the same VMware host server as the Contact Center virtual machine and the Avaya WebLM OVA. Alternatively, you can deploy the Avaya Aura[®] Media Server OVA standalone on a separate VMware host server.

*** Note:**

Avaya Aura[®] Media Server Element Manager displays licensing-related Critical Alarms until the Contact Center software is installed, configured, and licensed. The Contact Center software then pushes license keys to Avaya Aura[®] Media Server, clearing the licensing-related Critical Alarms.

Avaya Aura[®] Media Server OVA

The Avaya Aura[®] Media Server OVA contains information about the virtual machine server specification, operating system, and application software. This OVA contains the following components:

- Red Hat Enterprise Linux 7.x, 64-bit
- Avaya Aura[®] Media Server Release 8.0 software
- IP tables firewall file application
- VMware Tools. Do not update the VMware Tools software on this virtual machine unless instructed to do so by Avaya.

The Avaya Aura[®] Media Server OVA supports Business Continuity solutions.

Avaya Aura[®] Media Server is a software based media processing platform. Avaya Aura[®] Media Server provides the conference services required by SIP-enabled Contact Center.

The Avaya Aura® Media Server OVA package has the following default hardware configuration:

vCPU	Minimum CPU speed	Virtual memory required	Number of NICs	Virtual disk storage required	
4	2400 MHz	4.5 GB (4608 MB)	1 VMXNET3 Network Adapter	Size	50 GB
				Deploy the Avaya Aura® Media Server OVA using Thick Provision Lazy Zeroed. Avaya Aura® Media Server does not support thin provisioning.	

Contact Center does not support Avaya Aura® Media Server using these default deployment settings. After you deploy the Avaya Aura® Media Server, re-configure the virtual machine to have 4 or 8 CPUs and at least 8 GB RAM. Avaya Aura® Media Server is supported only on virtual machines with 4 or 8 CPUs.

In a virtualized Contact Center environment, you can use VMware to load the Avaya Aura® Media Server OVA package into a virtual machine in your contact center solution. The virtualized Contact Center server can then use the virtualized Avaya Aura® Media Server as a voice media processor.

Deploy the Avaya Aura® Media Server OVA using Disk Format - Thick Provision Lazy Zeroed. Avaya Aura® Media Server does not support thin provisioning.

Avaya Aura® Media Server OVA deployment procedures

About this task

This task flow shows you the sequence of procedures you perform to deploy the Avaya Aura® Media Server OVA.

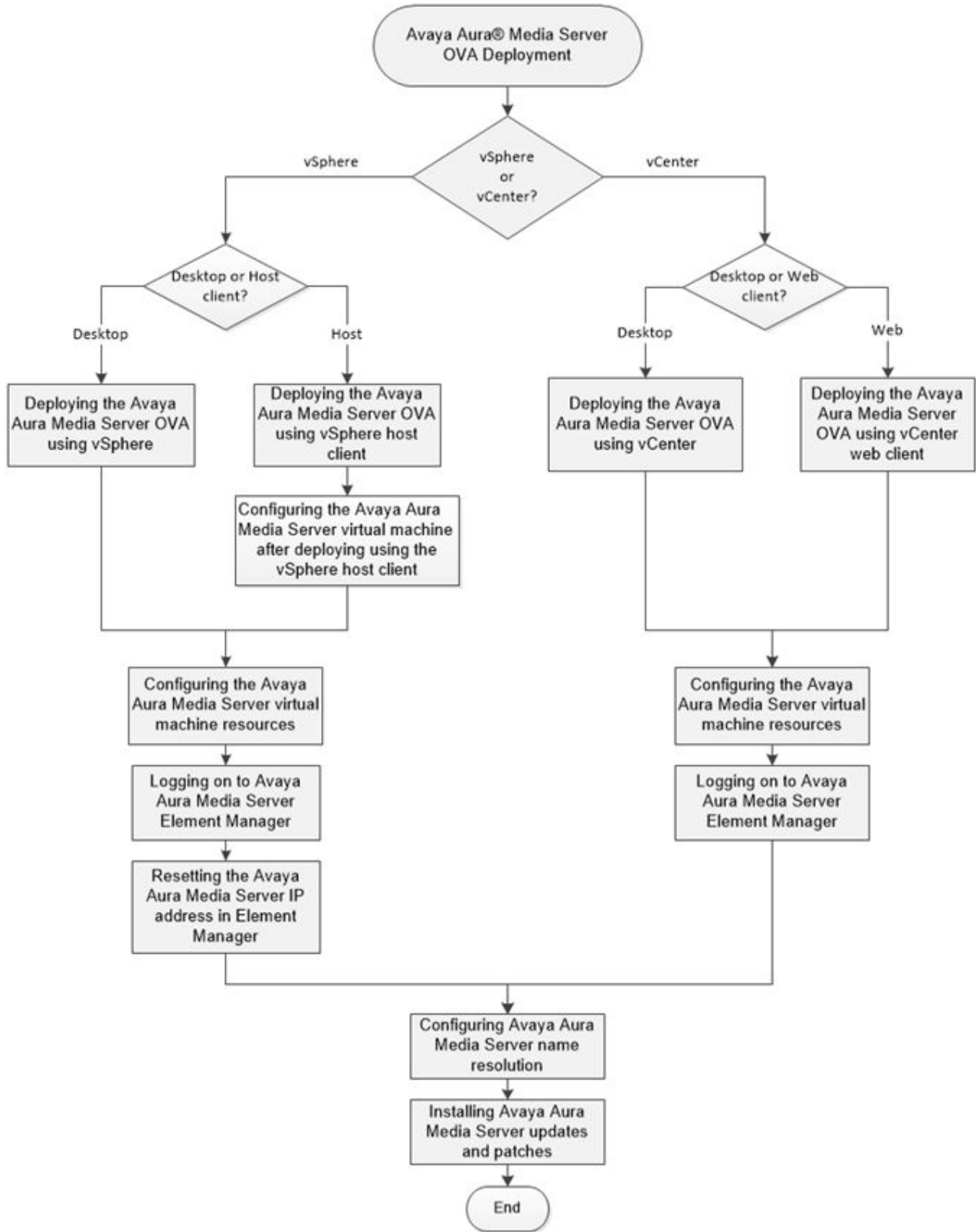


Figure 3: Avaya Aura® Media Server OVA deployment process

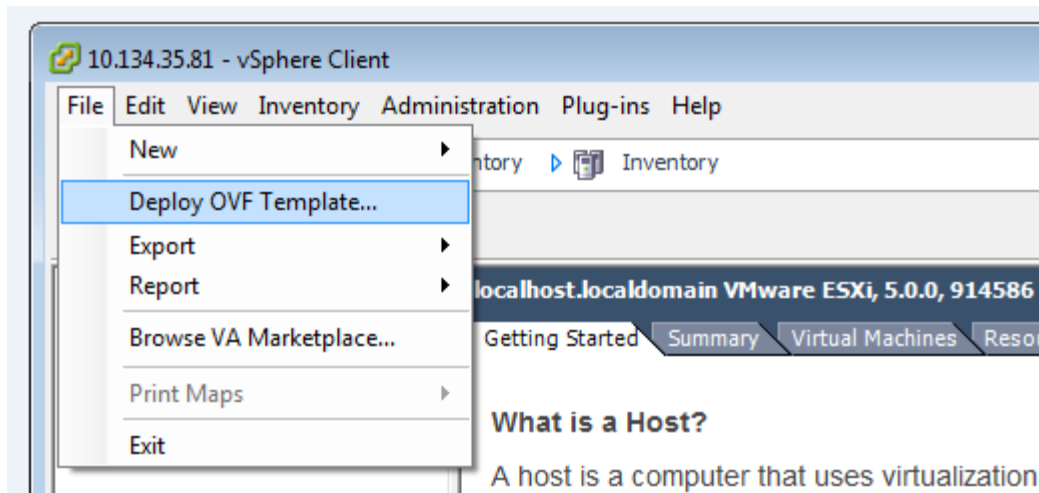
Deploying the Avaya Aura® Media Server OVA using vSphere (vSphere desktop client connected directly to ESXi host)

About this task

Deploy the Avaya Aura® Media Server OVA file onto a VMware ESXi host server. This creates a virtual machine with Avaya Aura® Media Server software for use in Contact Center solutions.

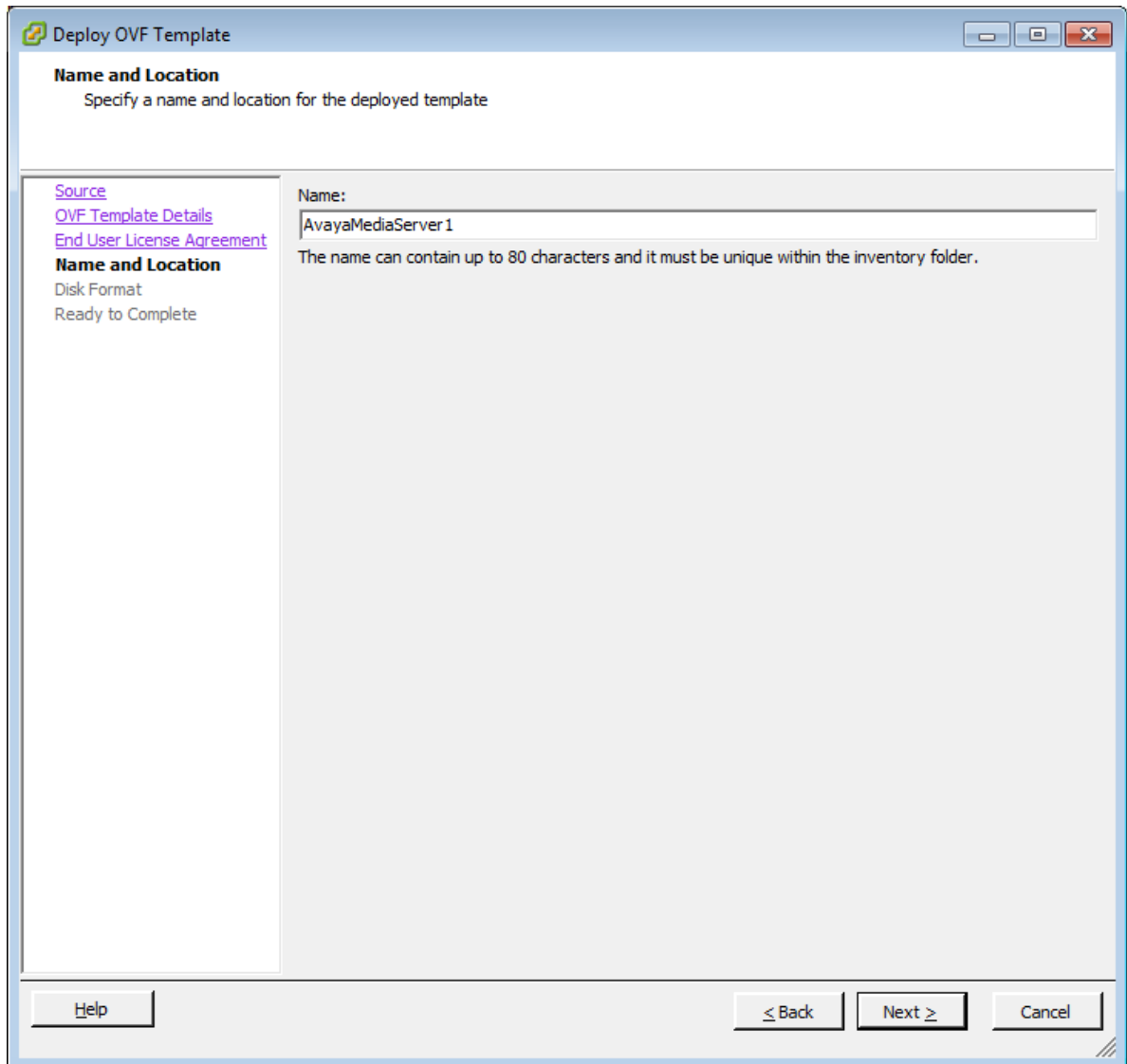
Procedure

1. In your vSphere client, select the ESXi host server.
2. Select **File > Deploy OVF Template**.



3. On the **Deploy OVF Template** window, click **Browse**.
4. On the **Open** message box, select Avaya Aura® Media Server OVA file.
5. Click **Open**.
6. On the **Deploy OVF Template** window, click **Next**.
7. On the **OVF Template Details** window, verify the details of the OVA template and click **Next**.
8. Read the **End User License Agreement** and click **Accept**.
9. Click **Next**.

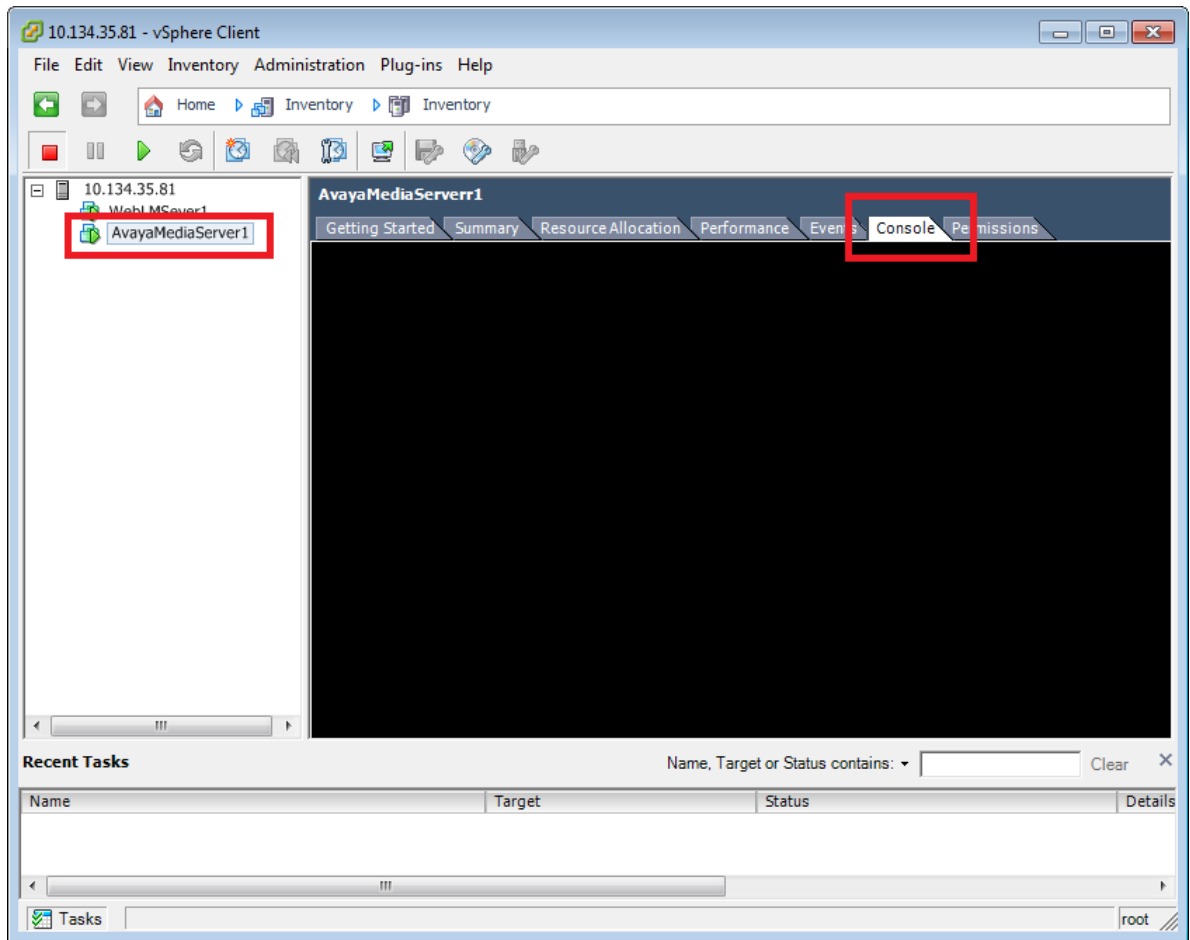
10. On the **Name and Location** window, type the name of the new Avaya Aura® Media Server virtual machine.



11. Click **Next**.
12. On the **Disk Format** window, select **Thick Provision Lazy Zeroed**.
13. Click **Next**.
14. On the **Ready to Complete** window, verify the deployment settings. If you need to modify any of the settings, click **Back**.
15. Click **Power on after deployment**.
16. Click **Finish**.

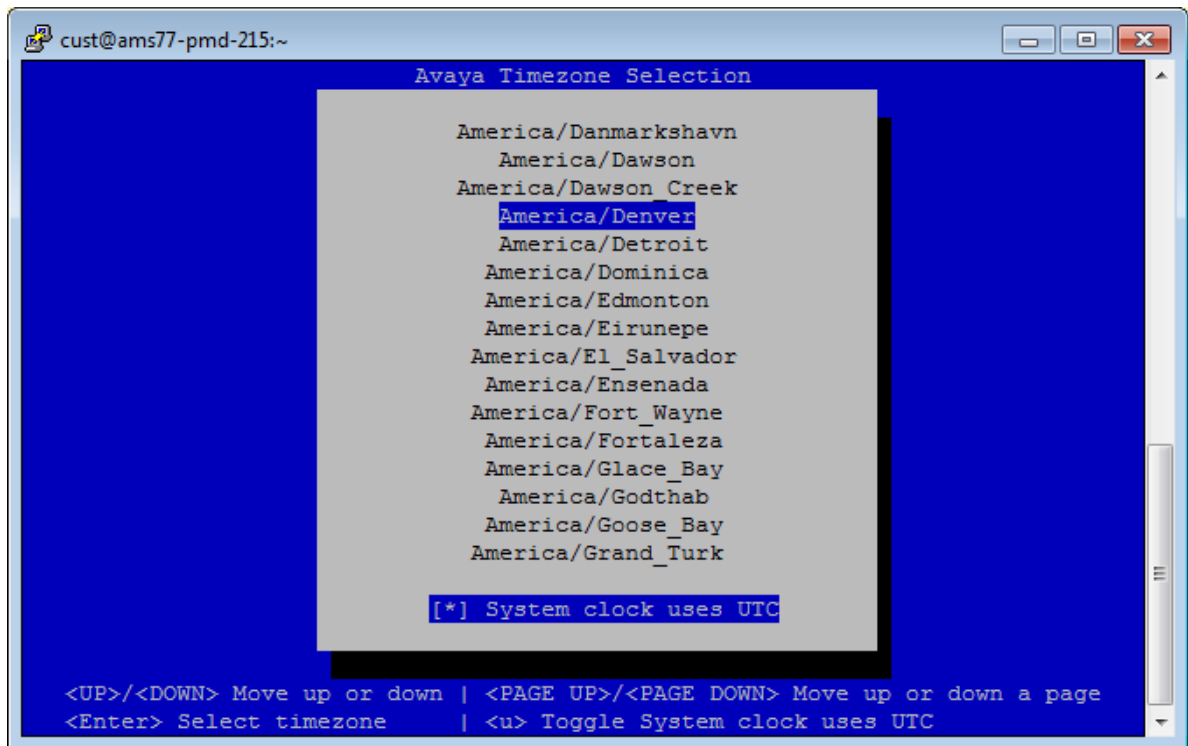
The Avaya Aura® Media Server template begins to load.

17. On the **Deployment Completed Successfully** message box, click **Close**.
18. In the vSphere client, from the inventory list in the left pane, select the new Avaya Aura® Media Server virtual machine.



19. In the right pane, select the **Console** tab for the Avaya Aura® Media Server virtual machine.
20. On the console, at the **login as** prompt, enter `cust`.
21. At the **Password** prompt, enter the password for the `cust` account.
22. At the command prompt, enter `netSetup`.
The Avaya Aura® Media Server appliance configuration utility starts.
23. Press `Enter` to continue.

24. From the list of time zones, select the time zone for the Contact Center solution.



25. To confirm selection and continue, press `c`.
26. At the **Enter Date** prompt, enter the date or press `Enter` to accept the displayed date.
27. At the **Enter Time** prompt, enter the time or press `Enter` to accept the displayed time.
28. To confirm selection and continue, press `c`.
29. At the **Enter server's hostname** prompt, enter the hostname of the Avaya Aura® Media Server virtual machine or press `Enter` to accept the displayed hostname.
30. At the **Enter server's IP address** prompt, enter the IP address of the virtual machine or press `Enter` to accept the displayed IP address.
31. At the **Enter netmask or prefix** prompt, enter the netmask IP address of the virtual machine or press `Enter` to accept the displayed IP address.
32. At the **Enter gateway IP address** prompt, enter the gateway IP address for the virtual machine or press `Enter` to accept the displayed IP address.
33. At the **Enter network domain** prompt, enter the domain name for the Avaya Aura® Media Server virtual machine or press `Enter` to accept the displayed domain. You must enter the domain name for the Contact Center solution.
34. At the **Enable static route (y/n)** prompt, enter `n`.
35. At the **Enter Primary DNS server IP address** prompt, enter the IP address of the primary DNS server or press `Enter` to accept the displayed IP address.

36. At the **Enter Secondary DNS server IP address** prompt, enter the IP address of the optional secondary DNS server or press `Enter` to accept the displayed IP address.
37. At the **Enable NTP Daemon (y/n)** prompt, enter `y` and then enter your NTP server details.
38. To confirm selection and continue, press `c`.

The Avaya Aura® Media Server appliance configuration utility updates the network details of the server.

39. Close the Avaya Aura® Media Server console.
40. Restart the Avaya Aura® Media Server virtual machine.

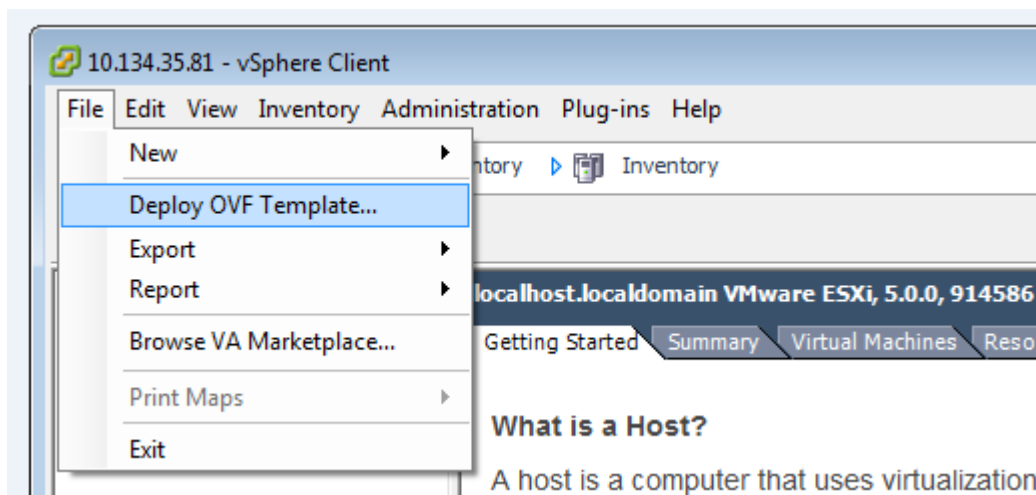
Deploying the Avaya Aura® Media Server OVA using vCenter (vSphere desktop client connected to vCenter)

About this task

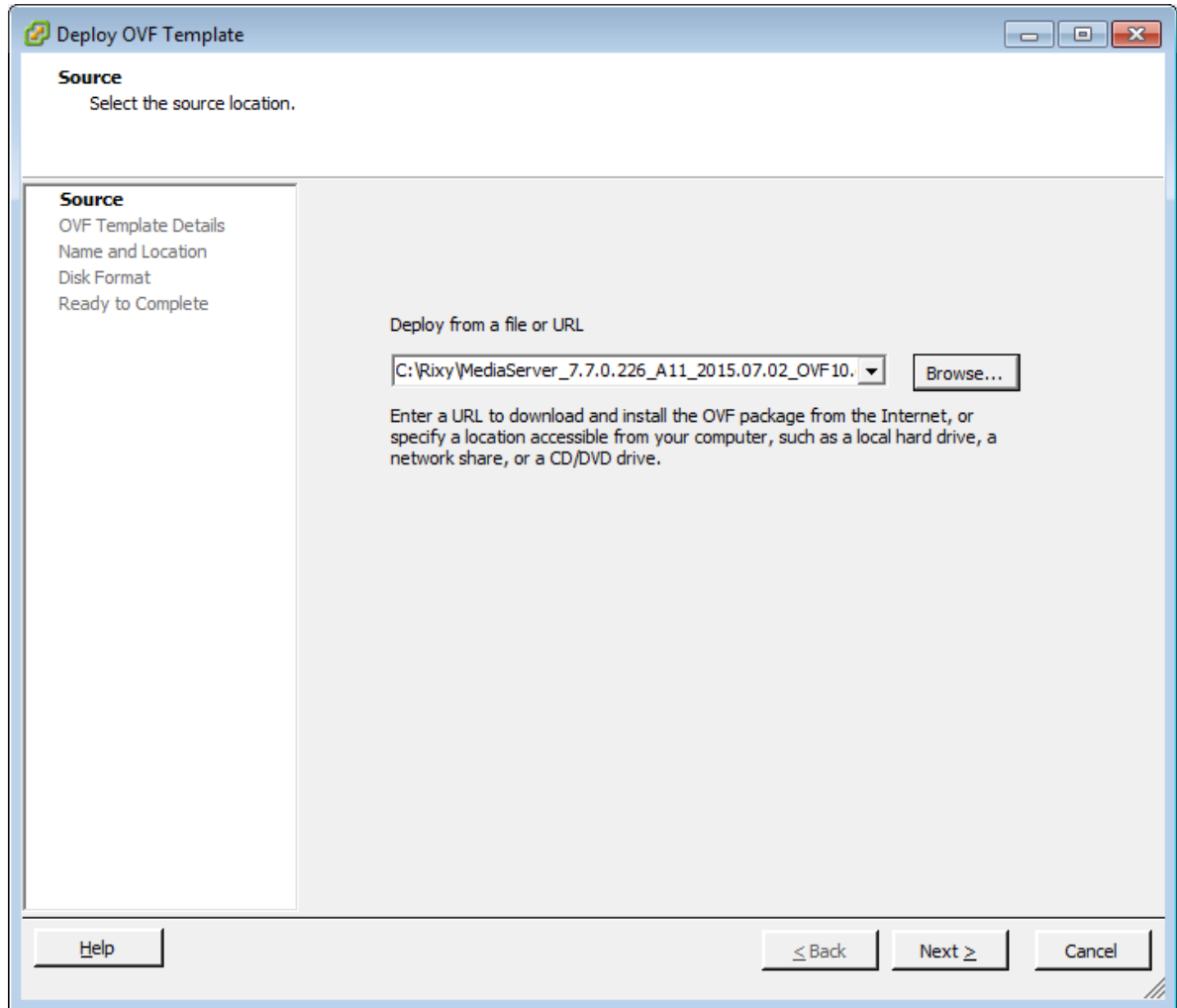
Deploy the Avaya Aura® Media Server OVA file onto a VMware ESXi host server using vCenter. This creates a virtual machine with Avaya Aura® Media Server software for use in Contact Center solutions.

Procedure

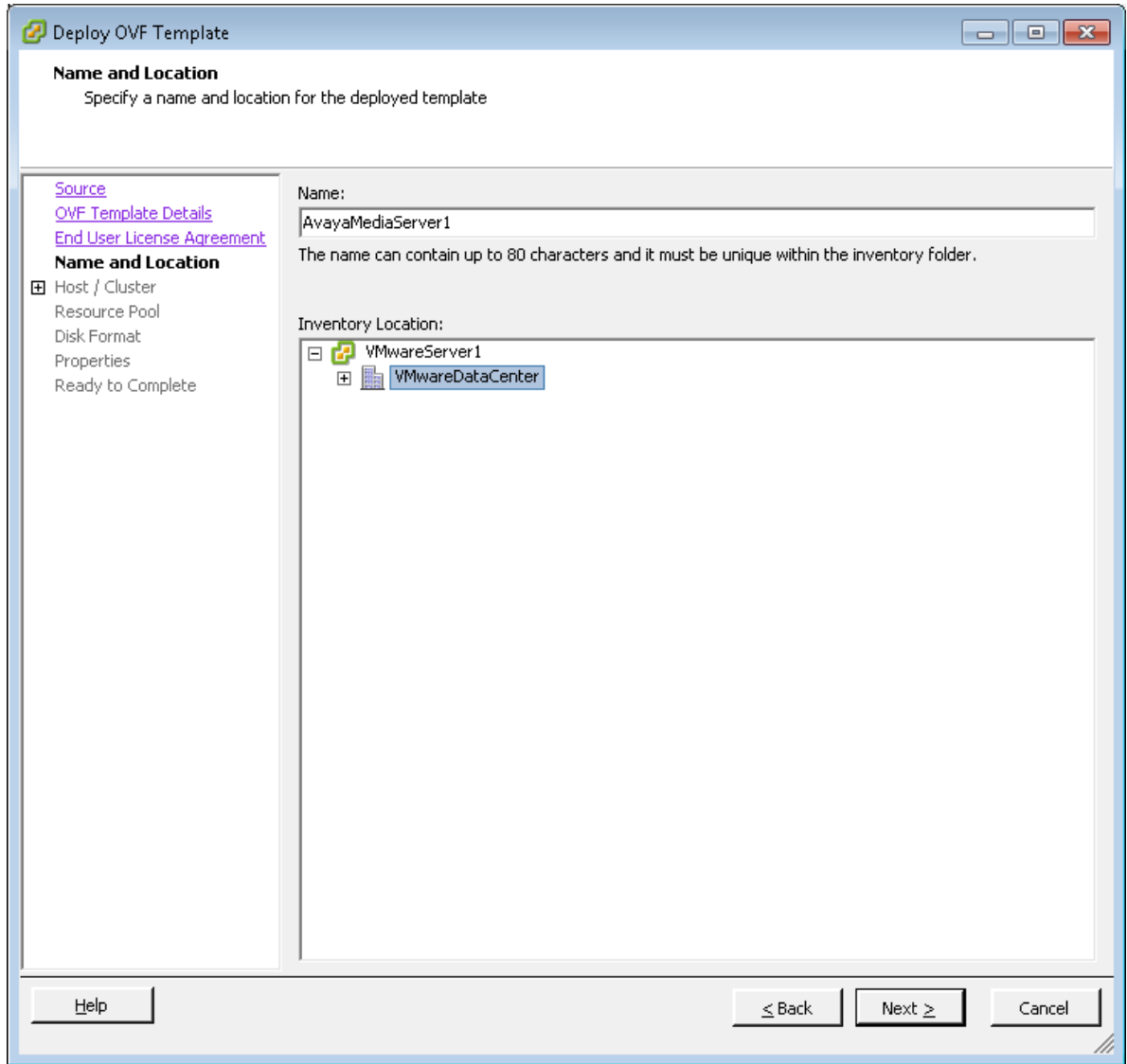
1. In your vCenter client, select the host server on which to deploy the Avaya Aura® Media Server OVA.
2. Select **File > Deploy OVF Template**.



3. On the **Source** window, click **Browse**.
4. On the **Open** message box, select the Avaya Aura® Media Server OVA file.
5. Click **Open**.

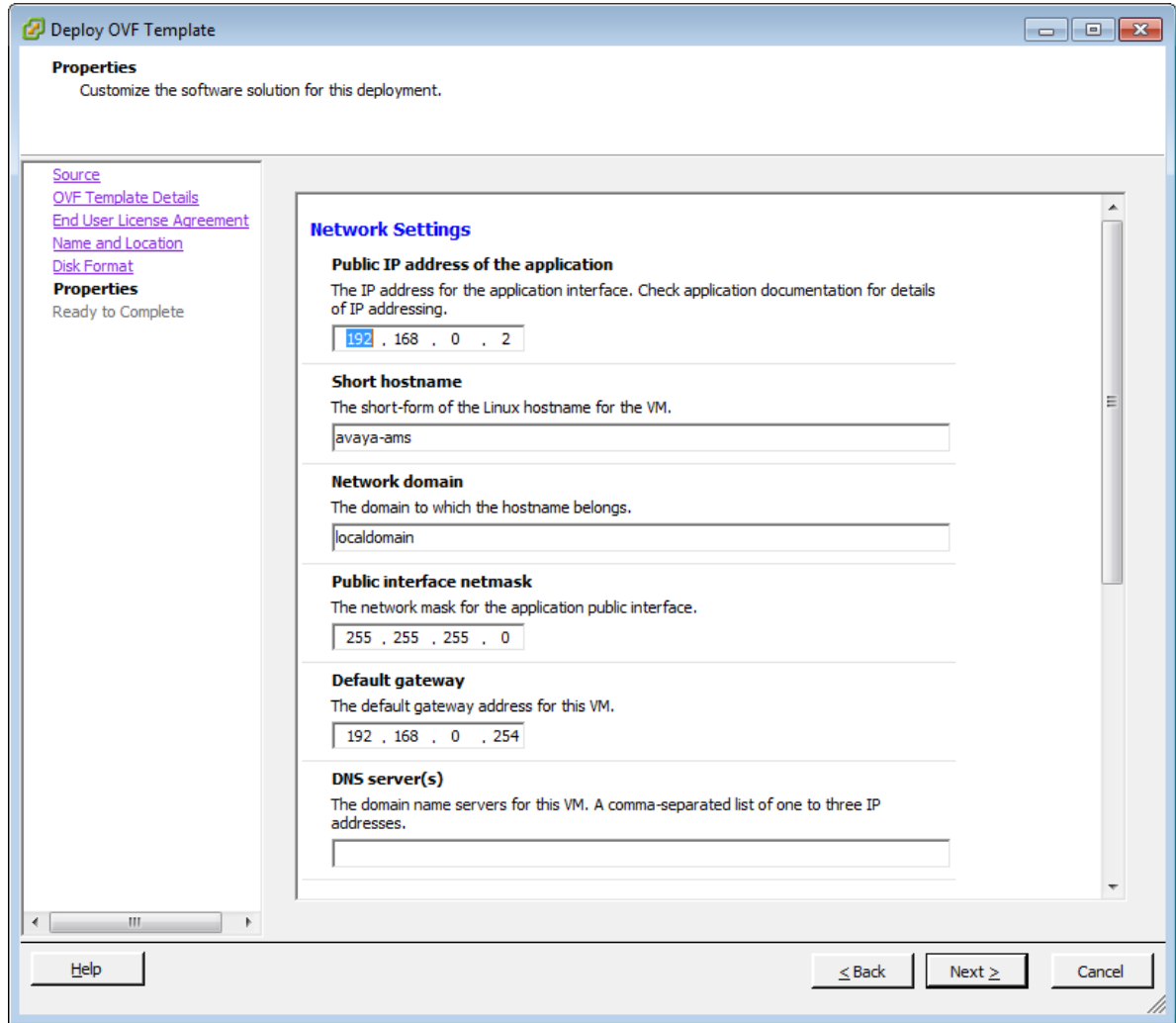


6. On the **Source** window, click **Next**.
7. On the **OVF Template Details** window, verify the details of the Avaya Aura® Media Server OVA template and click **Next**.
8. On the **End User License Agreement** window, read the license agreement, and if acceptable, click **Accept**.
9. Click **Next**.



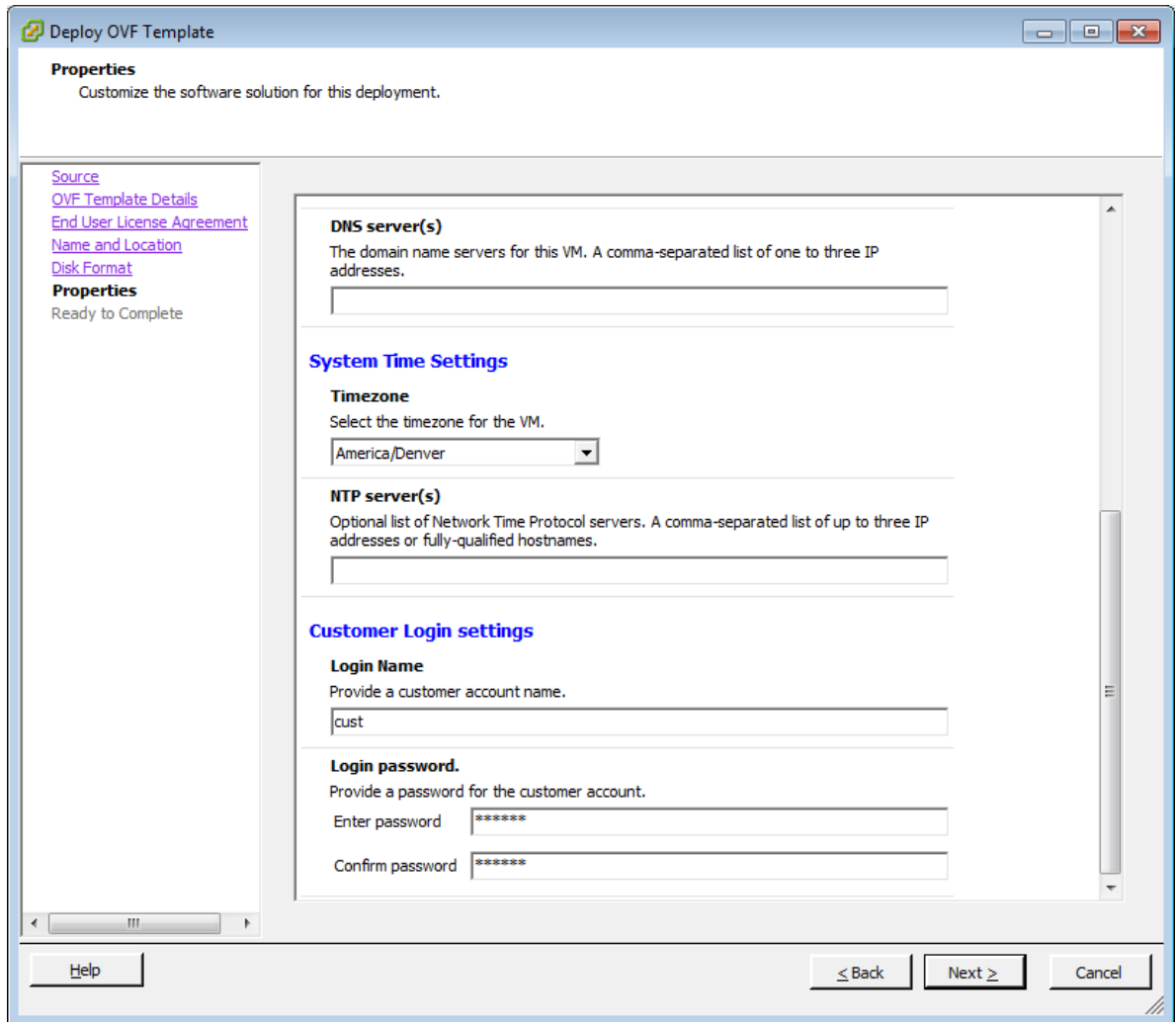
10. On the **Name and Location** window, type the name of the new Avaya Aura® Media Server virtual machine. This is not the server host name, this is the name of the VMware virtual machine as it appears in the VMware inventory.
11. Click **Next**.
12. On the Host and Cluster window, select the host server or cluster on which to deploy the Avaya Aura® Media Server OVA. If you selected a cluster, select a **Specific Host** on that cluster.
13. Click **Next** to display the **Storage** window.
14. From the **Select a destination storage for the virtual machine files** list, select a location to store the Avaya Aura® Media Server virtual machine image. Ensure that the storage location you select has sufficient available storage space to store a thick provisioned virtual machine image.

15. Click **Next**.
16. On the **Disk Format** window, select **Thick Provision Lazy Zeroed**. Avaya Aura® Media Server does not support thin provisioning in production environments.
17. Click **Next**.



18. On the **Properties** window, in the **Public IP address of the application** box, type the IP address of the Avaya Aura® Media Server server.
19. In the **Short hostname** box, type the name of the Avaya Aura® Media Server server.
20. In the **Network domain** box, enter the name of the domain used by Contact Center.
21. In the **Public interface netmask** box, type the subnet mask IP address.
22. In the **Default gateway** box, type the IP address of the default gateway.
23. In the **DNS server(s)** box, type the IP address of one or more DNS servers. Use IPv4 formatting. Separate the IP addresses with a comma.

24. On the **Properties** window, scroll down.



25. From the **Timezone** list, select the time zone for the solution.
26. In the **NTP server(s)** box, type the IP address of your Network Time Protocol (NTP) server. You use the NTP server to synchronize servers with each other and with the contact center solution. Use IPv4 formatting.
27. In the **Login Name** box, type the name of the customer account. The default name is `cust`.
28. In the **Enter password** box, type a password for the customer account.
29. In the **Confirm password** box, retype the password for the customer account.
30. Click **Next**.
31. On the **Ready to Complete** window, verify the deployment settings. If you need to modify any of the settings, click **Back**.
32. Click **Power on after deployment**.

33. Click **Finish**.

The Avaya Aura® Media Server template begins to load.

34. On the **Deployment Completed Successfully** message box, click **Close**.

Deploying the Avaya Aura® Media Server OVA using vSphere host client

About this task

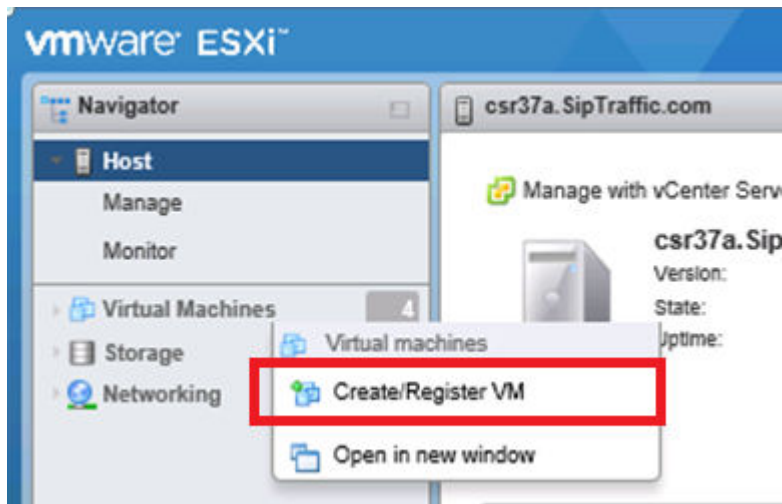
Deploy the Avaya Aura® Media Server OVA file onto a VMware ESXi host server. This creates a virtual machine with Avaya Aura® Media Server software for use in Contact Center solutions.

* Note:

The vSphere host client is a HTML5 client.

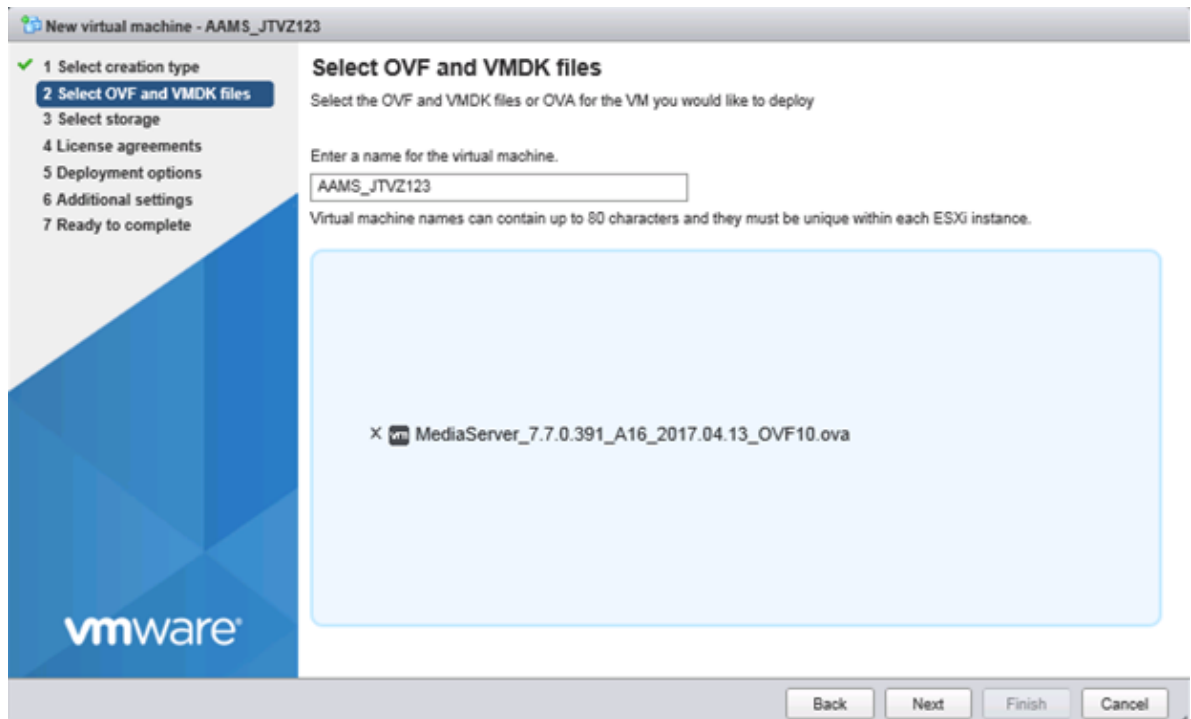
Procedure

1. In your vSphere host client, right-click on **Virtual Machines** and select **Create/Register VM**.



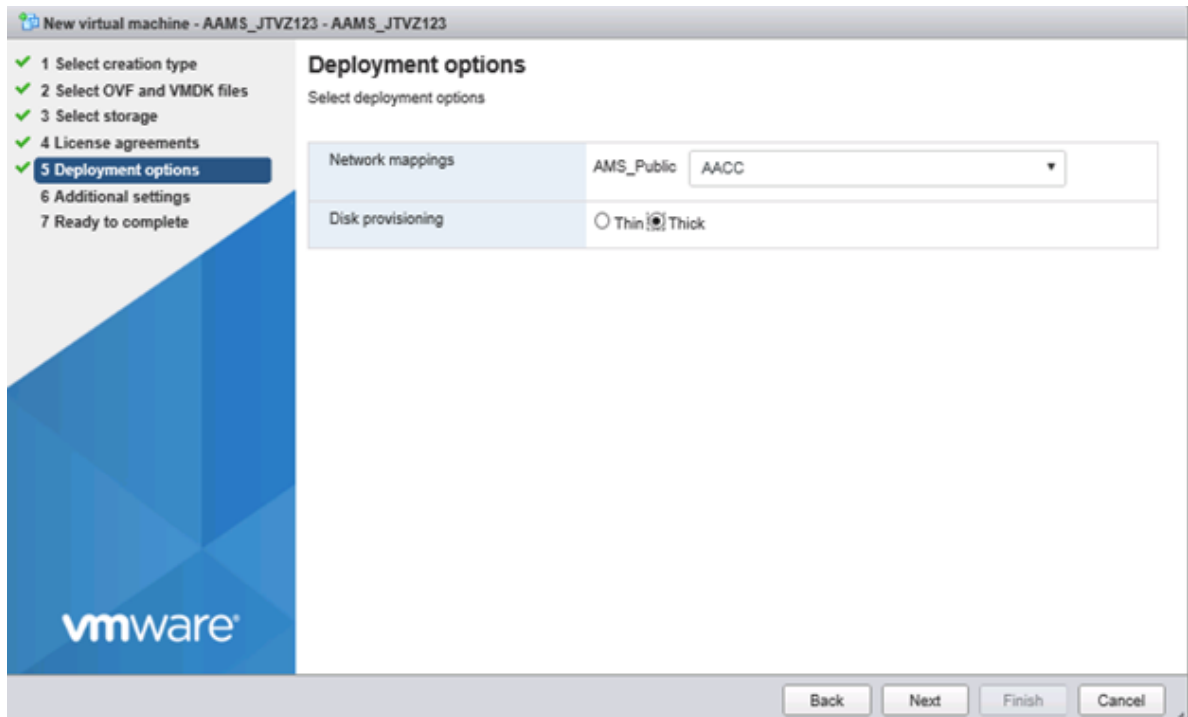
2. Under **Select creation type**, select **Deploy a virtual machine from an OVF or OVA file**.
3. Click **Next**.
4. Under **Select OVF and VMDK files**, type a name for the virtual machine.
5. Click **Browse** and select the Avaya Aura® Media Server OVA file.

6. Click **Next**.



7. Under **Select storage**, select a datastore location to store the Avaya Aura® Media Server virtual machine image. Ensure that the storage location you select has sufficient available storage space to store a thick provisioned virtual machine image.
8. Click **Next**.
9. Under **License agreements**, read the End User License Agreement and click **I agree**.
10. Click **Next**.

11. Under **Deployment options** , select the **Network mappings** and under Disk provisioning select **Thick**.



12. Click **Next**.
13. Under **Network Settings**, in the **Media Server IP address** box, type the IP address of the Avaya Aura® Media Server server.
14. In the **Short Hostname** box, type the name of the Avaya Aura® Media Server server.
15. In the **Network Domain** box, enter the name of the domain used by Contact Center.
16. In the **Media Server Netmask** box, type the subnet mask IP address.
17. In the **Default Gateway** box, type the IP address of the default gateway.
18. In the **DNS Servers** box, type the IP address of one or more DNS servers. Use IPv4 formatting. Separate the IP addresses with a comma.
19. Under **System Time Settings**, select the time zone for the solution from the **Timezone** list.
20. In the **NTP Servers** box, type the IP address of your Network Time Protocol (NTP) server. You use the NTP server to synchronize servers with each other and with the contact center solution. Use IPv4 formatting.
21. Under **Customer Login settings**, in the **Login Name** box, type the name of the customer account. The default name is `cust`.
22. In the **Login password** box, type a password for the customer account, and confirm the password.
23. Click **Next**.

24. Under **Ready to complete**, review and verify the deployment settings. If you need to modify any of the settings, click Back.
25. Click **Finish**.

 **Important:**

Do not refresh your browser while the VM is being deployed.

Next steps

When the Avaya Aura® Media Server OVA has been successfully deployed the virtual machine will be powered on automatically. If the virtual machine is not powered on automatically, power on the Avaya Aura® Media Server virtual machine.

After deploying the Avaya Aura® Media Server OVA using the vSphere host client, you might need to re-enter the configuration data after starting the Avaya Aura® Media Server virtual machine for the first time. If Avaya Aura® Media Server prompts you to configure the appliance after you start the virtual machine, then you must re-enter the configuration data. See [Configuring the Avaya Aura Media Server virtual machine after deploying using the vSphere Host Client](#) on page 97.

Deploying the Avaya Aura® Media Server OVA using vSphere web client

About this task

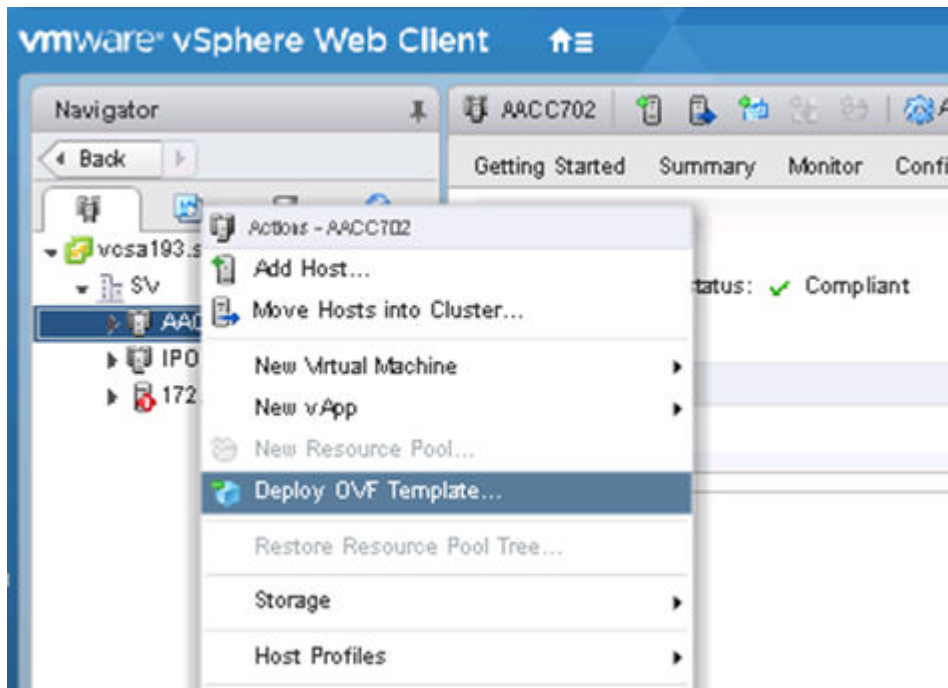
Deploy the Avaya Aura® Media Server OVA file onto a VMware ESXi host server. This creates a virtual machine with Avaya Aura® Media Server software for use in Contact Center solutions.

 **Note:**

The vSphere web client is supported with vCenter deployments only.

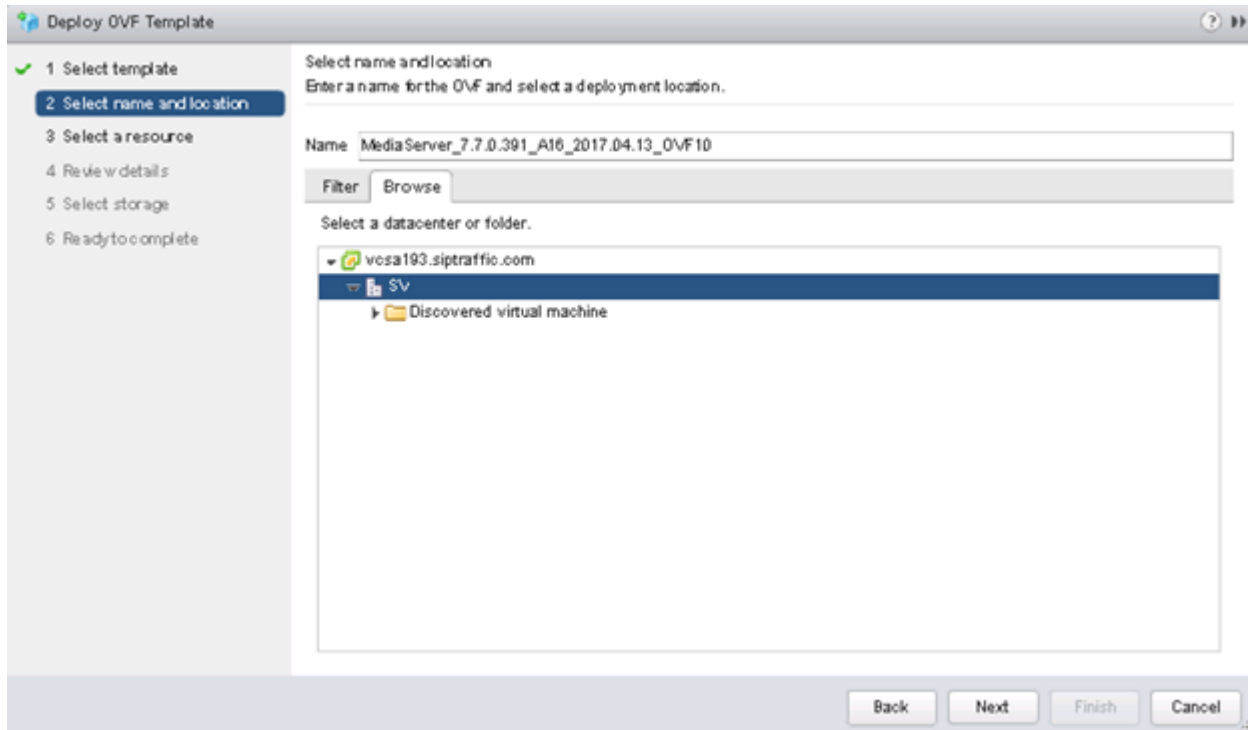
Procedure

1. In your vSphere web client, right-click in the **Navigator pane** and select **Deploy OVF Template**.



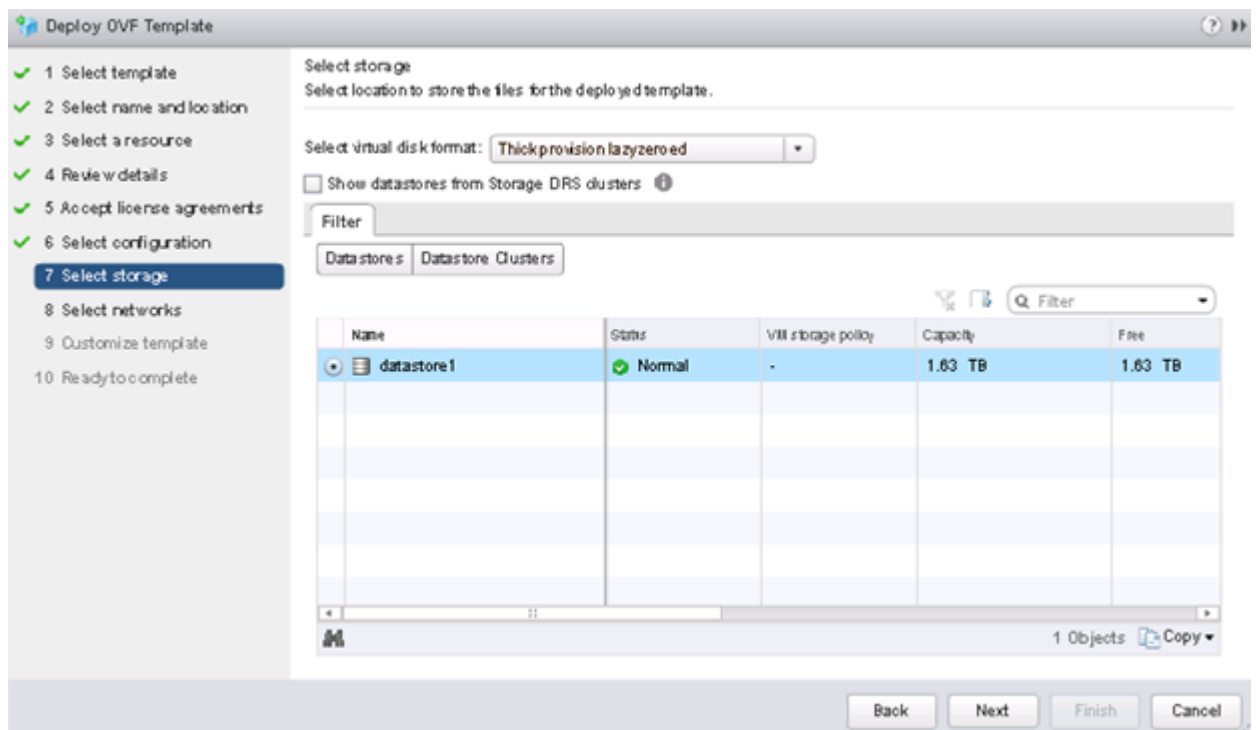
2. On the **Select template** page, select **Local file** and click **Browse** to select the Avaya Aura® Media Server OVA file.
3. Click **Next**.
4. On the **Select name and location** page, in the **Name** box, type a name for the virtual machine.

5. Select a datacenter location for the Avaya Aura® Media Server virtual machine.



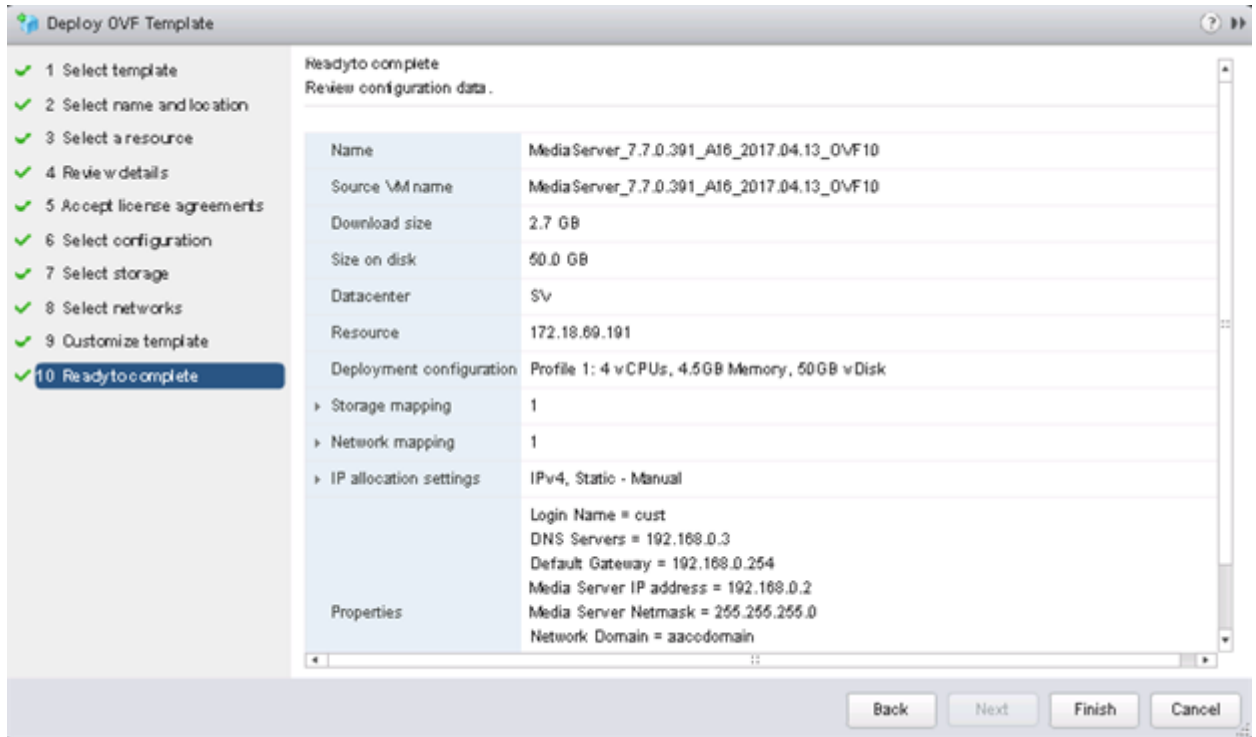
6. Click **Next**.
7. On the **Select a resource** page, navigate to and select the host where you want to deploy the Avaya Aura® Media Server virtual machine.
8. Click **Next**.
9. On the **Review details** page, review the Avaya Aura® Media Server details.
10. Click **Next**.
11. On the **Accept license agreements** page, read the license agreement and click **Accept**.
12. Click **Next**.
13. On the **Select configuration** page, accept the default profile 1 with 4 vCPU, 4.5GB Memory, and 50GB vDisk.
14. Click **Next**.
15. On the **Select storage** page, from the **Select virtual disk format** drop-down list, select **Thick provision lazy zeroed**.

16. Select a location to store the Avaya Aura® Media Server virtual machine image. Ensure that the storage location you select has sufficient available storage space to store a thick provisioned virtual machine image.



17. Click **Next**.
18. On the **Select networks** page, select the destination network for the Avaya Aura® Media Server virtual machine from the drop-down list.
19. Click **Next**.
20. On the **Customize template** page, under **Customer Login settings**, type the name of the customer account in the **Login Name** box. The default name is `cust`.
21. In the **Login password** box, type a password for the customer account, and confirm the password.
22. Under **Network Settings**, in the **DNS Servers** box, type the IP address of one or more DNS servers. Use IPv4 formatting. Separate the IP addresses with a comma.
23. In the **Default Gateway** box, type the IP address of the default gateway.
24. In the **Media Server IP address** box, type the IP address of the Avaya Aura® Media Server server.
25. In the **Media Server Netmask** box, type the subnet mask IP address.
26. In the **Network Domain** box, enter the name of the domain used by Contact Center.
27. In the **Short Hostname** box, type the name of the Avaya Aura® Media Server server.

28. Under **System Time Settings**, in the **NTP Servers** box, type the IP address of your Network Time Protocol (NTP) server. You use the NTP server to synchronize servers with each other and with the contact center solution. Use IPv4 formatting.
29. From the **Timezone** list, select the time zone for the solution.
30. Click **Next**.
31. Under **Ready to complete**, review and verify the deployment settings. If you need to modify any of the settings, click **Back**.



32. Click **Finish**.

! Important:

Do not refresh your browser while the VM is being deployed.

Next steps

When the Avaya Aura® Media Server OVA has been successfully deployed, power on the virtual machine.

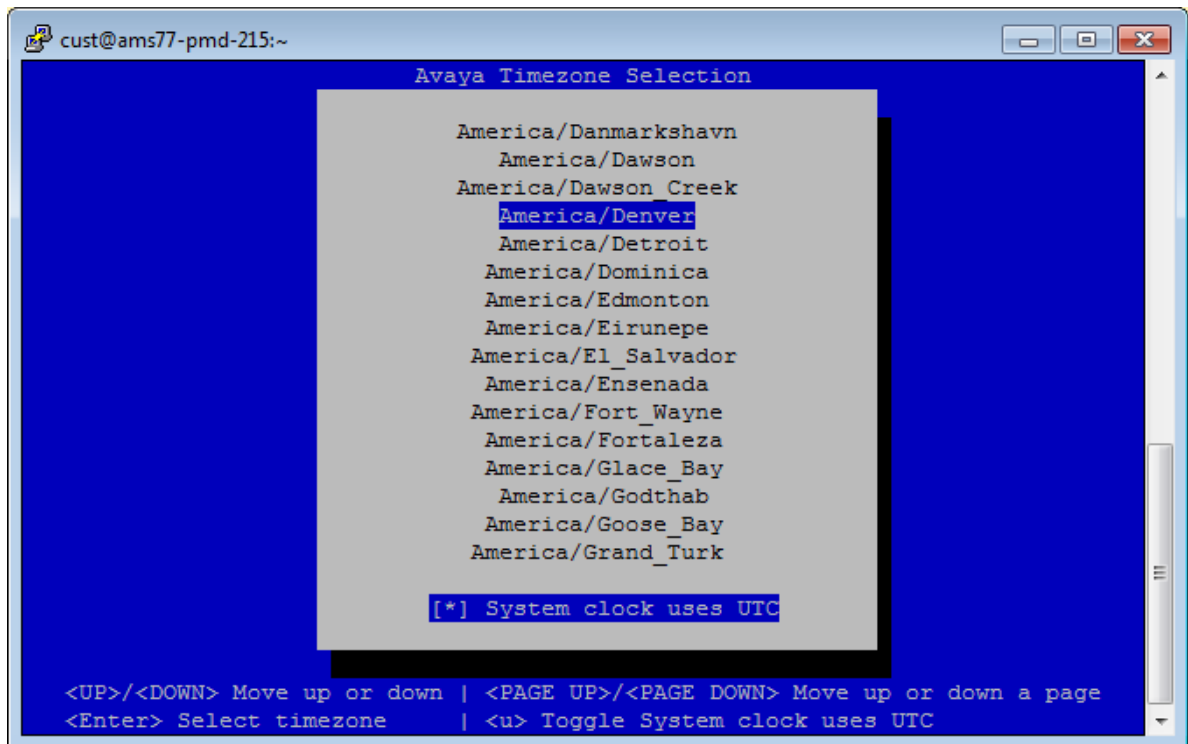
Configuring the Avaya Aura® Media Server virtual machine after deploying using the vSphere Host Client

About this task

After you power on the Avaya Aura® Media Server virtual machine for the first time, enter the Avaya Aura® Media Server configuration data.

Procedure

1. Connect to the Avaya Aura® Media Server virtual machine, after you power on the virtual machine for the first time.
2. When the **Do you wish to configure this appliance now? y/n** prompt appears, type **Y** and press **Enter**.
3. From the list of time zones, select the time zone for the Contact Center solution.



4. To confirm selection and continue, press **c**.
5. At the **Enter Date** prompt, enter the date or press **Enter** to accept the displayed date.
6. At the **Enter Time** prompt, enter the time or press **Enter** to accept the displayed time.
7. To confirm selection and continue, press **c**.
8. At the **Enter server's hostname** prompt, enter the hostname of the Avaya Aura® Media Server virtual machine or press **Enter** to accept the displayed hostname.

9. At the **Enter server's IP address** prompt, enter the IP address of the virtual machine or press `Enter` to accept the displayed IP address.
10. At the **Enter netmask or prefix** prompt, enter the netmask IP address of the virtual machine or press `Enter` to accept the displayed IP address.
11. At the **Enter gateway IP address** prompt, enter the gateway IP address for the virtual machine or press `Enter` to accept the displayed IP address.
12. At the **Enter network domain** prompt, enter the domain name for the Avaya Aura® Media Server virtual machine or press `Enter` to accept the displayed domain. You must enter the domain name for the Contact Center solution.
13. At the **Enable static route (y/n)** prompt, enter `n`.
14. At the **Enter Primary DNS server IP address** prompt, enter the IP address of the primary DNS server or press `Enter` to accept the displayed IP address.
15. At the **Enter Secondary DNS server IP address** prompt, enter the IP address of the optional secondary DNS server or press `Enter` to accept the displayed IP address.
16. At the **Enable NTP Daemon (y/n)** prompt, enter `y` and then enter your NTP server details.
17. Verify the details entered. If you need to update any of the details, press `u`.
18. To confirm selection and continue, press `c`.
19. At the **Enter Login ID** prompt type the name of the customer account to configure. The default account name is `cust`.
20. At the **New password** prompt, type a password for the customer account.
21. Confirm the password.
22. To confirm selection and continue, press `c`.

The Avaya Aura® Media Server appliance configuration utility updates the details of the server.
23. Restart the Avaya Aura® Media Server virtual machine.

Configuring the Avaya Aura® Media Server virtual machine resources

About this task

Configure the VMware resources of the Avaya Aura® Media Server virtual machine. A virtual machine cannot have more vCPUs than the maximum number of physical CPUs on the host virtual server platform.

Avaya Aura® Media Server supports only a 4 vCPU or 8 vCPU virtual machine. You must set the *CPU — Resource Allocation* of the virtual machine to match the vCPU count. For Contact Center deployments, Avaya Aura® Media Server must have at least 8GB of memory.

To adjust the virtual machine *Resource Allocations*, you must power off the virtual machine.

*** Note:**

This is a generic procedure for configuring the required resources for the virtual machine. There are interface differences depending on the VMware configuration client you are using. Refer to VMware documentation for more information about configuring virtual machine resources.

Before you begin

- Monitor the performance of the virtual machine.
- Review the following documents to determine the required resource values for your deployment type:
 - For AACC solutions, see *Avaya Aura® Contact Center Overview and Specification*.
 - For ACCS solutions, see *Avaya Contact Center Select Solution Description*.

Procedure

1. Locate the virtual machine in the VMware inventory, and shut down the guest.
2. Right-click on the virtual machine and select **Edit Settings**.
3. Set the CPU (total number of cores) count to the required number of CPUs for your deployment type. Set the number of cores per socket to 1.
4. Set the CPU Resource Reservation value to the required MHz value for your deployment.
5. Set the Memory value to the required memory value for your deployment.
6. Set the Memory Reservation value to the required memory reservation value for your deployment.
7. Save your changes.
8. Power on the virtual machine.
9. Continue to monitor the performance of the Avaya Aura® Media Server virtual machine.

Logging on to Avaya Aura® Media Server Element Manager

About this task

Log in to Avaya Aura® Media Server Element Manager to configure Avaya Aura® Media Server.

Element Manager (EM) is a web-based administration tool that facilitates the Operation, Administration, and Maintenance (OAM) of Avaya Aura® Media Server.

*** Note:**

You must have more than one Avaya Aura® Media Server account managed by separate users. If one account is disabled or lost, another account can perform critical tasks, backups or recovery. For more information, see *Implementing and Administering Avaya Aura® Media Server*.

Procedure

1. On your client computer, start a Web browser.
2. In the address box, enter `https://SERVER_IP_ADDRESS:8443/em`. Where `SERVER_IP_ADDRESS` is the IP address of the Avaya Aura® Media Server.
3. In the **User ID** box, type the Avaya Aura® Media Server User ID log in account name. For example, type `Admin`.
4. In the **Password** box, type the account password.
5. Click **Sign In**.

Resetting the Avaya Aura® Media Server IP address in Element Manager

About this task

When you change the Avaya Aura® Media Server IP address, the Avaya Aura® Media Server database still contains the old IP address. You must update the IP address in Element Manager.

Procedure

1. Log on to Avaya Aura® Media Server Element Manager with administrative privileges.
2. In the left pane, select **System Configuration > Network Settings > IP Interface Assignment**.
3. Under **IPv4 Interfaces**, set the **Signaling**, **Media**, and **Cluster** boxes to the IP address of the Avaya Aura® Media Server server.
4. Click **Save**.

Configuring Avaya Aura® Media Server name resolution

About this task

Configure Avaya Aura® Media Server to resolve the hostname and Fully Qualified Domain Name (FQDN) of the Contact Center Manager Administration server. The Contact Center Manager Administration (CCMA) software is installed on the Contact Center server.

Procedure

1. Log in to Element Manager with administrative privileges.
2. Navigate to **EM > System Configuration > Network Settings > Name Resolution**.
3. Click **Add**.
4. In the **IP Address** box, enter the Contact Center Manager Administration IP address.
5. In the **Hostname** box, enter the Contact Center Manager Administration hostname.
6. Click **Save**.

Installing Avaya Aura® Media Server updates and patches on a virtual machine

Before you begin

- Download and review the Contact Center Release Notes. The Release Notes contain the known issues, patches, and workarounds specific to a release and patch line-up of Contact Center. For more information about the Contact Center Release Notes, see <http://support.avaya.com>.
- Download the most recent Avaya Aura® Media Server patches and store them in a local subdirectory on your client computer.
- Backup the Avaya Aura® Media Server before applying patches.

About this task

Install a new update or patch to apply a change to an Avaya Aura® Media Server virtual machine. Contact Center cannot process contacts while Avaya Aura® Media Server patches or updates are installing.

Note:

Follow the instructions in the Contact Center Release Notes and in each Avaya Aura® Media Server patch Readme file.

Note:

You can update the Avaya Aura® Media Server software appliance RHEL operating system and other underlying lower-level software. Contact Center cannot process contacts while these Avaya Aura® Media Server System Layer updates are installing. For more information, see *Deploying and Updating Avaya Aura® Media Server Appliance* on the Avaya Support website at <https://support.avaya.com>.

Procedure

1. Navigate to the Element Manager for the Avaya Aura® Media Server node you want to patch.
2. In the navigation pane, click **Tools > Manage Software > Updates > Upload Updates**.

3. Click **Browse** to select the software update to upload.

The selected file must be an official Avaya Aura® Media Server update package in ISO or ZIP format.

4. Click **Upload**.

Your browser shows a progress spinner until the upload completes.

The web page refreshes when the update completes and displays the details of the update including the filename of the uploaded file.

5. Determine if you need to use the Quick Fix Engineering (QFE) procedure by performing the following steps:

- a. In the navigation pane, click **Tools > Manage Software > Manage Updates**.
- b. Expand the **Details** section of the update by clicking on the down arrow button.
- c. Review the list of updates. If only QFEs are listed as **Ready for Installation**, then stop using this procedure and perform the QFE installation procedure instead. For more information on installing QFEs, refer to the QFE Readme and to the upgrading and patching documentation.

6. Prevent new sessions from starting on the system. In the Element Manager navigation pane, click **System Status > Element Status** and select **More Actions > Pending Lock**.

7. Click **Confirm**.

8. Check for active sessions on the server. In the Element Manager navigation pane, click **System Status > Monitoring > Active Sessions**.

Wait for the active sessions to end. If you continue before all active sessions end, then the system ends the remaining active sessions

9. Lock Avaya Aura® Media Server and end any remaining sessions. In the Element Manager navigation pane, click **System Status > Element Status** and select **More Actions > Lock**.

10. Click **Confirm**.

11. After the system ends all the sessions, stop Avaya Aura® Media Server. In the navigation pane, click **System Status > Element Status**.

12. Click **Stop** and confirm the operation on the following page.

13. Click **Tools > Manage Software > Updates > Upload Updates**.

14. Click **Browse**, and browse to the local subdirectory where you downloaded the patches.

15. Select the update to apply to Avaya Aura® Media Server.

If you downloaded a System Layer update, apply this first.

16. Click **Upload**.

17. If you have multiple updates to apply, repeat [step 14](#) on page 102 to [step 16](#) on page 102 until all updates are complete.

18. When the patch application is complete, click **Tools > Manage Software > Inventory**.
19. Verify the patch version listed in the **Patch Level** column is correct.
20. Select **System Status > Element Status**, and click **Start**.
21. Click **Confirm**.
22. In the Element Manager navigation pane, click **System Status > Element Status** and select **More Actions > Unlock**.
23. Click **Confirm**.
24. Select **System Status > Alarms** and check for service-impacting alarms.

Chapter 9: Avaya Contact Center Select virtual machine deployment

Create a VMware virtual machine and then install Avaya Contact Center Select application software on it to build an Avaya Contact Center Select virtual machine.

Avaya Contact Center Select virtual machine

Use the Avaya Contact Center Select virtual machine to provide context-sensitive and skill-based routing for customer voice and multimedia contacts.

The Avaya Contact Center Select virtual machine contains the following contact center application software.

- Contact Center Manager Server (CCMS)
- Contact Center Manager Administration (CCMA)
- Communication Control Toolkit (CCT)
- Contact Center Multimedia (CCMM)
- Contact Center License Manager (LM)
- Contact Center Manager Server Utility (SU)
- Orchestration Designer (OD)
- Default Avaya Contact Center Select configuration data
- Firewall policy
- An Ignition Wizard configuration utility
- Avaya Workspaces (optional)

To create the Avaya Contact Center Select virtual machine, perform the following:

1. Create a VMware virtual machine that meets or exceeds the minimum specifications for your solution. For information about engineering the VMware resources for your Software Appliance, refer to *Avaya Contact Center Select Solution Description*.
2. Install the Windows Server 2012 Release 2, Windows Server 2016, or Windows Server 2019 Standard or Datacenter edition English operating system on the virtual machine.

3. License and activate the Microsoft Windows 2012 R2, Windows Server 2016, or Windows Server 2019 operating system.
4. Configure the server and format the hard disk partitions to the required specifications.
5. Install VMware Tools on the server.
6. Download and read the most recent Avaya Contact Center Select Release Notes.
7. Obtain an Avaya Contact Center Select DVD or ISO image.
8. Download the most recent Avaya Contact Center Select Service Packs and updates.
9. Obtain an Avaya Contact Center Select license file.
10. Use the Avaya Contact Center Select DVD or ISO image to install the *Avaya Contact Center Select without Avaya Aura Media Server* software. **Note:** The *Avaya Contact Center Select with Avaya Aura Media Server* install option does not support VMware.
11. Use the Avaya Contact Center Select Configuration Ignition Wizard to rapidly deploy a functional contact center solution.
12. Continue to monitor the VMware real-time resources.

You can use any account with local administrative rights to install Avaya Contact Center Select. You can use any account with local administrative rights to upgrade and patch Avaya Contact Center Select; you do not need to always use the same account to perform these tasks.

! **Important:**

You must disable the Admin Approval Mode security feature on the Contact Center server. This ensures that accounts with local administrative rights get full privileges for running applications on the Contact Center server.

The Avaya Contact Center Select virtual machine has the following minimum hardware characteristics:

vCPU	Minimum CPU speed	Virtual memory reservation	Hard disk space	Number of NICs
4 (Depending on the required deployment size of the ACCS 7.1)	2400 MHz	16 to 20 GB (Depending on the required deployment size of the ACCS 7.1)	See Contact Center virtual machine hard disks and partitions on page 115.	1 VMXNET3 Network Adapter

Each Avaya Contact Center Select virtual machine requires a Linux-based Avaya Aura® Media Server. Each Avaya Contact Center Select virtual machine also requires an additional, separate, Avaya WebLM licensing manager server.

If you want to configure Avaya Workspaces as part of your Avaya Contact Center Select solution, you must deploy one additional Avaya Workspaces virtual machine using the Avaya Workspaces OVA, with the following hardware characteristics:

vCPU	Minimum CPU speed	Virtual memory reservation	Hard disk space	Number of NICs
8	2400 MHz	32 GB	500 GB	1 VMXNET3 Network Adapter

Server Operating Systems:

The procedures in this chapter include installing the server Operating Systems (OS) required by Avaya Contact Center Select software applications. You must complete a fresh install of the OS for each Contact Center installation. Do not install Contact Center applications on an existing OS from which you uninstalled either Contact Center or other software applications.

Downloading the most recent documentation

Before you begin

- Download the most recent version of Acrobat Reader.
- Access the Avaya website at <http://support.avaya.com>.

About this task

Download the most recent documentation to ensure you have the most recent updates. Updates in the documentation accurately reflect the most recent changes in the software.

Procedure

1. Log on to the Avaya website.
2. Compare the versions of the documentation on the site with the versions you have.
3. If the version number on <http://support.avaya.com> is higher than your version, download the latest version of the document.
4. Review the Avaya website for release notes and readme files.

Creating a VMware virtual machine for Contact Center software

About this task

Create a VMware virtual machine for the Contact Center application software.

Note:

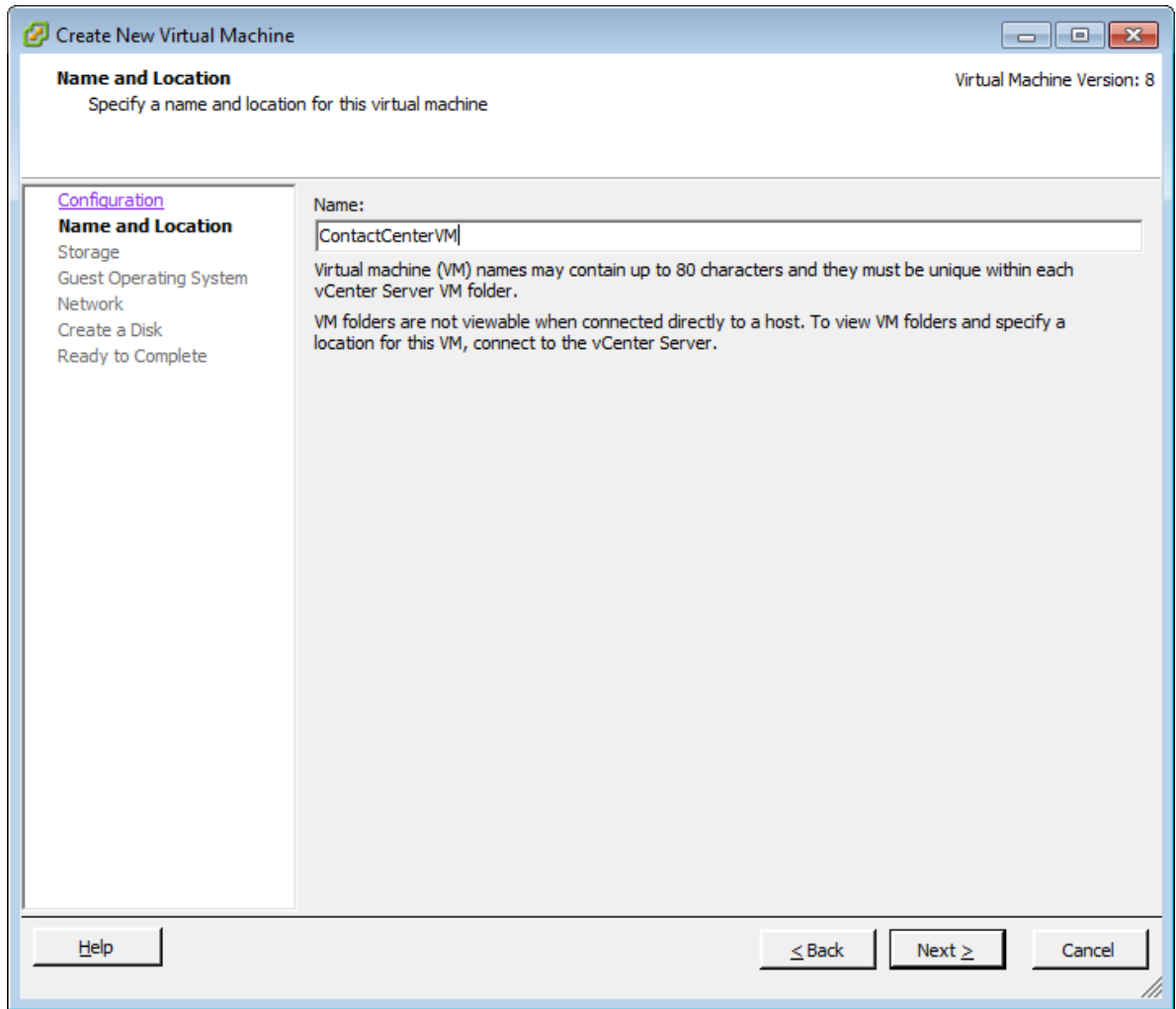
When creating virtual machines for deploying Contact Center, ensure that the custom VMware setting *SMBIOS.reflectHost* is either absent, or, if present, is set to False. If this setting is set

to True, it can break the installation of the Contact Center software. Installations of the Contact Center software with `SMBIOS.reflectHost=True` are not supported.

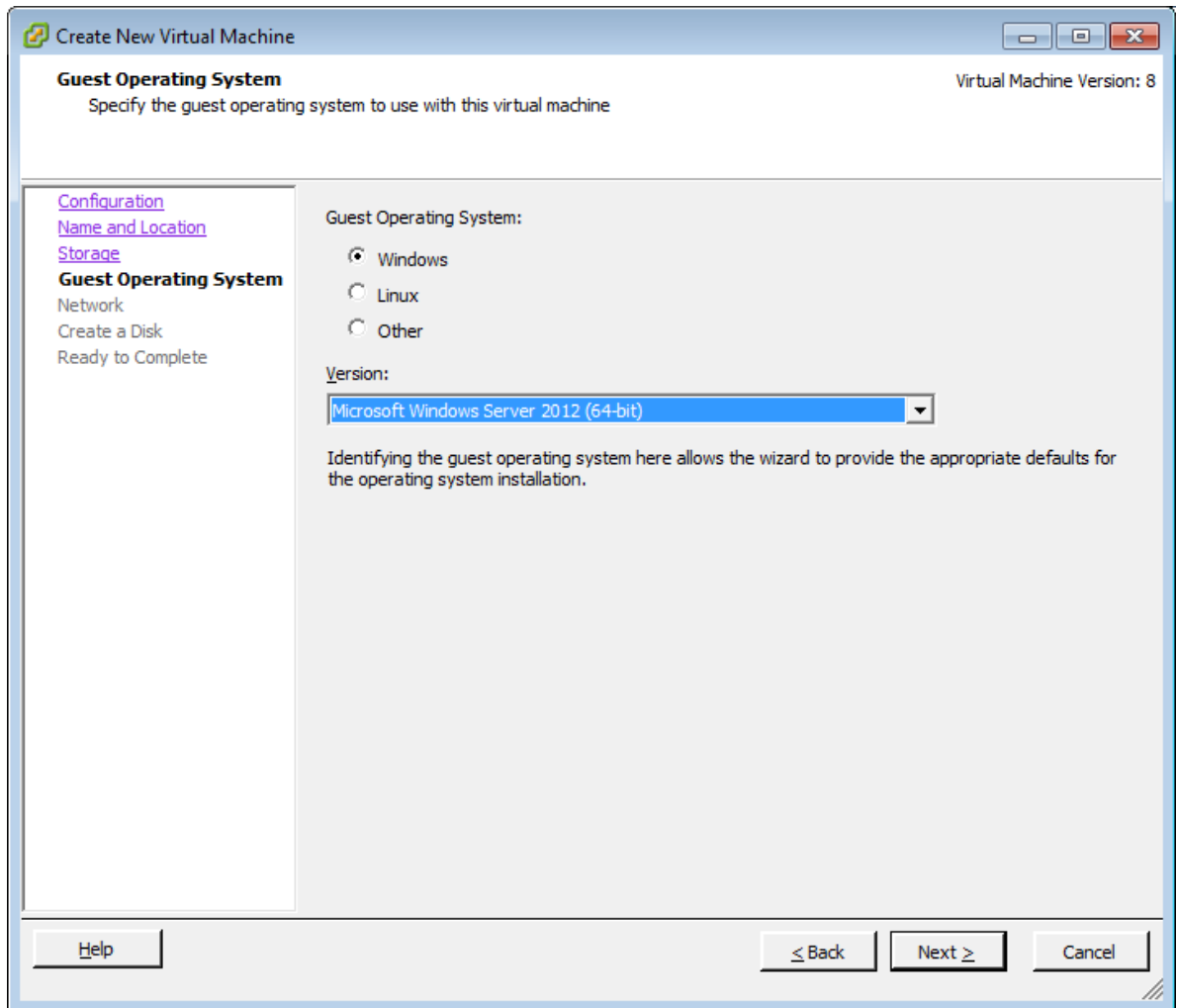
Procedure

1. Read *Performance Best Practices for VMware vSphere* for the version of VMware you are using.
2. Read your server hardware provider's documents covering virtualization support.
3. Obtain server hardware that meets the Contact Center host hardware specification and supports VMware vSphere.
4. Install the most recent Basic Input/Output System (BIOS) or Unified Extensible Firmware Interface (UEFI) available for your host server.
5. On the VMware host server, disconnect or disable unused or unnecessary physical hardware devices such as: COM ports, LPT ports, USB controllers, network interfaces, storage controllers.
6. On the host server, enable all available Virtualization Technology options in the hardware. The available virtualization settings vary by hardware provider and BIOS or UEFI version. Read your hardware provider's documents covering virtualization support to determine which settings to configure.
7. Configure the server hardware and firmware settings to select system performance over power savings.
8. Install VMware vSphere software on your host server.
9. Configure a networking infrastructure on the host server. Configure a VM Network and a Standard Switch (vSwitch).
10. Using the vSphere client, create a new virtual machine for Contact Center. Using vSphere client, select **File > New > Virtual Machine**.

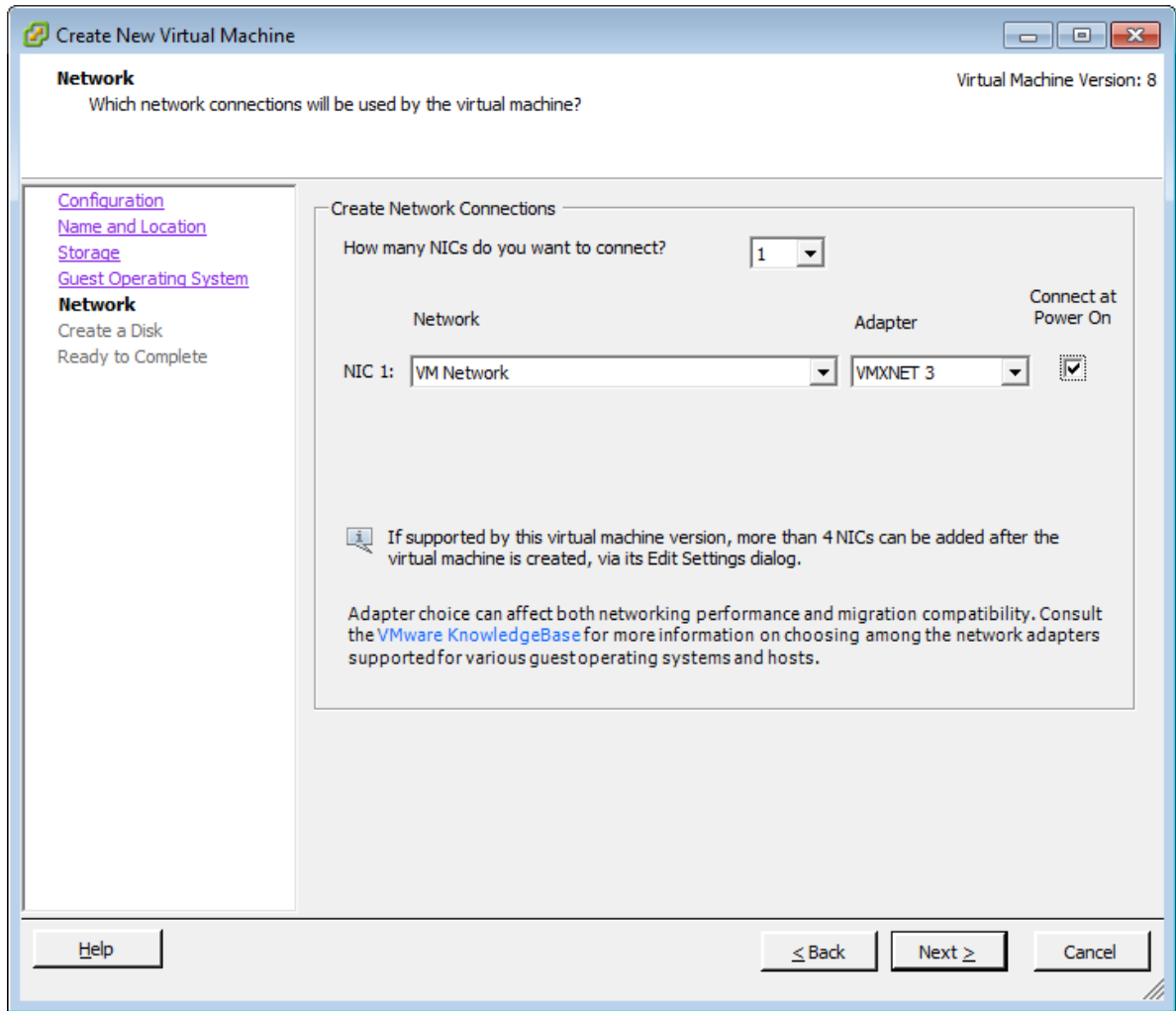
11. Give the virtual machine a descriptive **Name**.



12. On the **Guest Operating System** tab, select **Microsoft Windows Server 2012 (64-bit)**, **Microsoft Windows Server 2016 (64-bit)**, or **Microsoft Windows Server 2019 (64-bit)**.

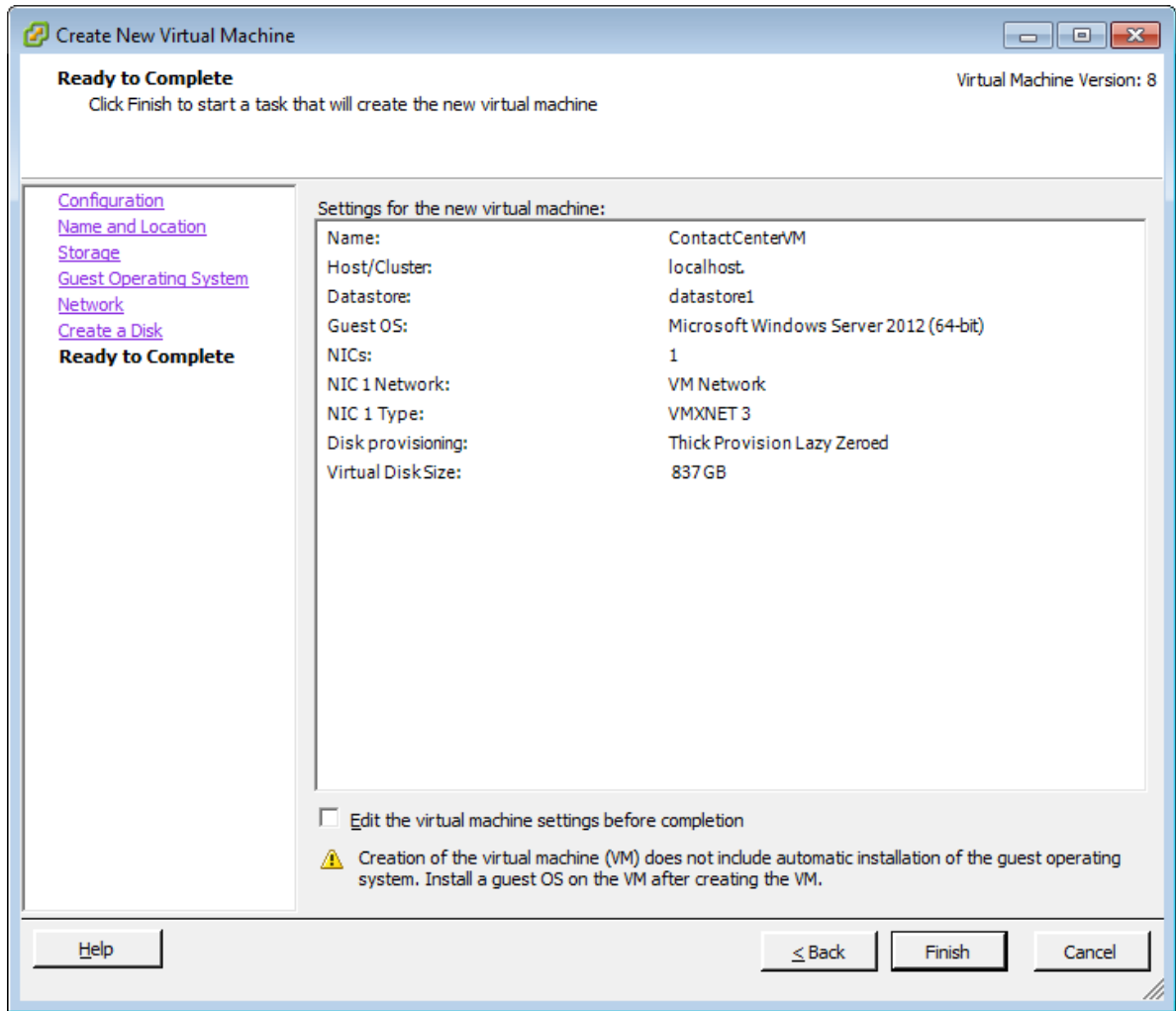


13. Configure and use VMXNET 3 networking.

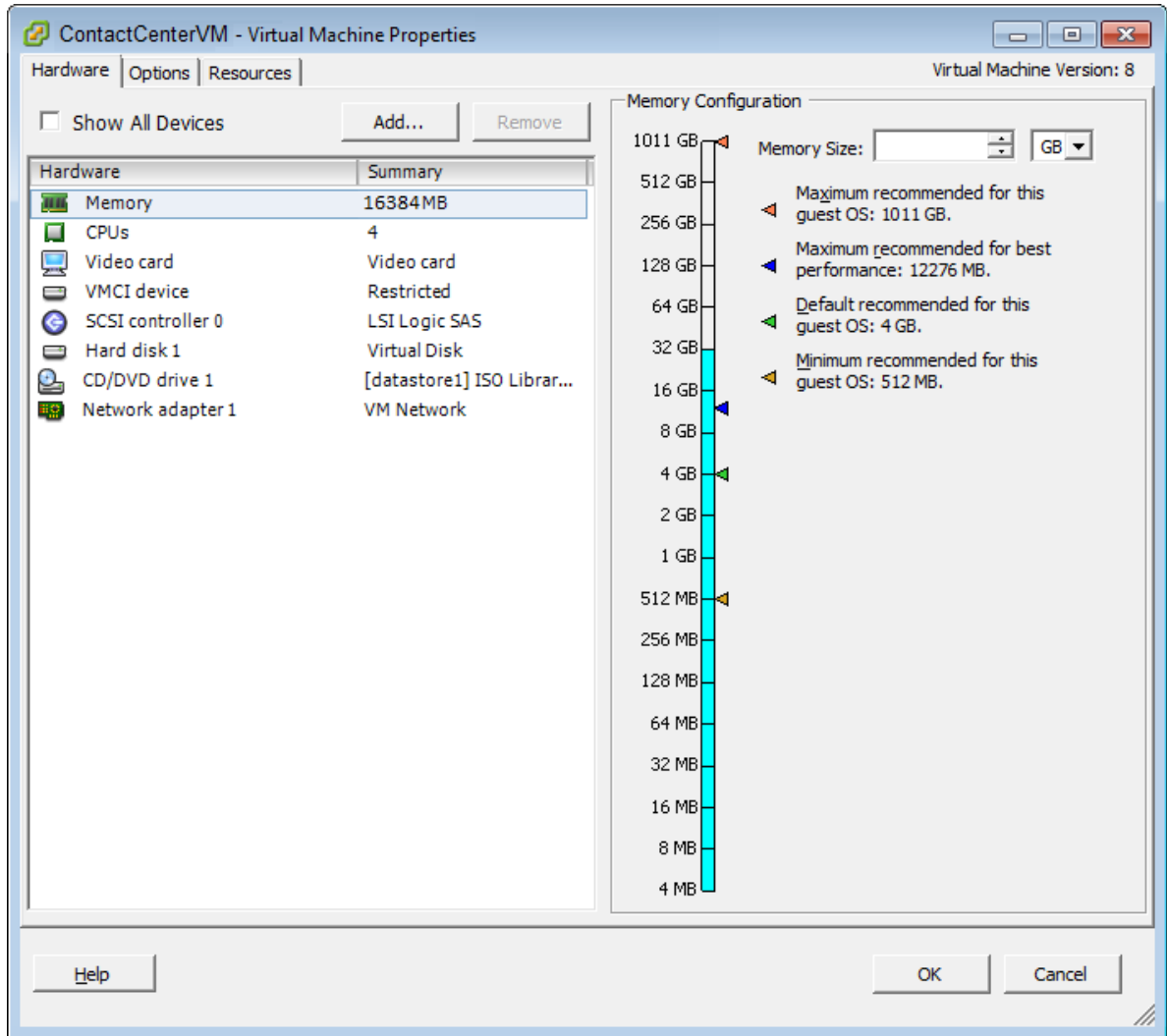


14. Configure the virtual disk space using **Thick Provision Lazy Zeroed**. Contact Center does not support thin provisioning.

15. Review your configuration before creating the virtual machine.



16. Configure the virtual machine with the CPU, memory, and disk space required for your Contact Center configuration.



17. On each virtual machine, completely disable time synchronization to the host time.

During commissioning, you set the operating system to synchronize time from the Domain Name Server (DNS).

18. Add the Microsoft Windows Server 2012 Release 2, Microsoft Windows Server 2016, or Microsoft Windows Server 2019 DVD image to the vSphere ISO library. Configure the virtual machine **CD/DVD drive 1** to use this Windows Server ISO image.
19. Using vSphere client, turn on the virtual machine and prepare to install the operating system software.

Installing Microsoft Windows Server 2012 R2

Before you begin

- Ensure that you have a newly formatted server that meets the specifications in *Avaya Contact Center Select Solution Description* on which to install Microsoft Windows Server 2012 R2.

Do not upgrade your operating system. Contact Center is not supported on an upgraded operating system.

- Configure all servers for RAID as described in *Avaya Contact Center Select Solution Description*.
- Ensure that you have a DVD for Microsoft Windows Server 2012 R2 *Standard* or *Data Center*. Ensure that your DVD is the R2 version of Windows Server 2012 *Standard* or *Data Center*.
- Ensure that you have a Microsoft Windows Server 2012 R2 operating system product key.
- Know the IP address and network details for this Contact Center server.

About this task


Install the Microsoft Windows Server 2012 R2 *Standard* or *Data Center* operating system and configure it to support Contact Center server software.

The following table lists some of the main inputs to consider while installing the operating system.

Name	Description
Computer name	Do not use spaces or underscores or exceed 15 characters. The name must start with an alphabetic character. Server names must adhere to RFC1123. Avaya recommends that you configure the server final production name before installing Contact Center software. The computer name must match (including case sensitivity) the DNS name.
Disk drives	Format the partitions as required for the server. For more information, see <i>Avaya Contact Center Select Solution Description</i> .
Domain name	Configure as required for your site. You must check to ensure the DNS Domain name (including case) matches the server name if the server is added to a domain after configuration.
Licensing modes	Select Per server licensing mode.
Network components	Configure IP Address, WINS, and DNS for the network cards as per configuration. Contact Center does not support IPv6.
Network connections	If the server has more than one NIC/adaptor, ensure contact center subnet appears first in the network adapter binding order.
Hard Disk Partitions	Configure C: drive to be a primary drive. Configure the other drives on your server to meet the requirements listed below.

Procedure

1. Insert the Microsoft Windows Server 2012 R2 *Standard* or *Data Center* DVD into the DVD drive.

2. Turn on the power to the server.
The server begins to boot up.
3. On the **Windows Setup** screen, select a **Language to install** from the list.
4. Select a **Time and currency format** from the list.
5. Select **Keyboard or input method** from the list.
6. Click **Next**.
7. Click **Install now**.
8. Depending on the DVD image that you use, you might need to select an operating system from a list. Select a version of Microsoft Windows Server 2012 R2 *Standard* or *Data Center* that includes a Graphical User Interface (GUI). Install a version that includes “**(Server with a GUI)**”.
9. Click **Next**.
10. On the **Enter the product key to activate Windows** window, enter the operating system product key.
11. Click **Next**.
12. On the **Windows Setup** screen, read the terms of the license agreement and select **I accept the license terms**.
13. Click **Next**.
14. Select **Custom: Install Windows only (advanced)** to install a clean new installation of the operating system.
15. Select the disk partition on which you want to install Microsoft Windows Server 2012 R2.
 **Important:**
You can use the partition management options to configure the partitions on your server.
16. Click **Next**.
The installation proceeds and automatically restarts the server several times.
17. After completing the installation, log on to the server as Administrator. Enter and confirm the Administrator password.
18. Select **Set time zone** and complete the information as required for your system.
19. Select **Configure Networking** and complete the information for your Network Interface Card (NIC) with the server IP address.
20. Select **Provide computer name and domain** and complete the information for your server name and network settings.
21. Change the DVD drive letter to E: to ensure the correct drive letters are free for the Contact Center application and database hard disk drives and partitions.

22. Install other required drivers for your hardware configuration.
23. Configure the hard disk drives and partitions for this server using the Microsoft Windows Server 2012 R2 Computer Manager - Disk Management utility.

Contact Center virtual machine hard disks and partitions

Create individual virtual hard disks for each of the required partitions for your Contact Center virtual machine. When creating a virtual hard disk for the Operating System partition, create a hard disk size 1GB greater than the required partition size to accommodate the creation of any additional Windows partitions which might be created automatically as part of the Windows Server install.

For example, for an Operating System partition size requirement of 80GB, create an 81GB virtual hard drive. For each additional Contact Center required partition, create a virtual hard drive greater than or equal to the partition size requirement. The virtual hard disk must be of sufficient size such that when the associated partition is created and formatted it has a size matching the required partition size for the install.

For improved multimedia offline data retention, Avaya recommends using a 600 GB partition for multimedia storage. The multimedia 600 GB partition requires SAN Storage.

Table 1: Contact Center Virtual Machine hard disk minimum partition sizes

Hard disk drive partition description	Drive letter	Minimum partition sizes	Recommended partition sizes, 300 GB multimedia partition	Recommended partition sizes, 600 GB multimedia partition
Operating System drive	C:	80 GB NTFS partition	80 GB NTFS partition	80 GB NTFS partition
Application drive	D:	100 GB NTFS partition	120 GB NTFS partition	120 GB NTFS partition
DVD drive	E:	—	—	—
Voice Contact Server database drive	F:	180 GB NTFS partition	200 GB NTFS partition	200 GB NTFS partition
Multimedia Contact Server database drive	G:	200 GB NTFS partition	300 GB NTFS partition	600 GB NTFS partition
Database journal drive	H:	80 GB NTFS partition	100 GB NTFS partition	100 GB NTFS partition
	Total	641 GB of Thick Provisioned disk space in a VMware datastore.	801 GB of Thick Provisioned disk space in a VMware datastore.	1101 GB of Thick Provisioned disk space in a SAN datastore.

If using 900 GB Raid–1 disks, use the above Minimum Partition size option.

Contact Center requires Hardware RAID-1 with duplicate hard disk drives with identical specifications. Therefore, the VMware host server must implement Hardware RAID-1 or better.



Navigating the Microsoft Windows Server 2012 R2 User Interface

This section describes how to navigate between the main user interface screens of the Windows Server 2012 R2 operating system.

The following table describes some of the main Microsoft Windows Server 2012 R2 user interface screens.

Screen name	Description
Start	The Start screen contains shortcuts to the main administration interfaces of the server. If you have an application that you access on a regular basis, you can add it to the Start screen so that it's more immediately accessible. The Start screen displays the currently logged on user and provides some basic server log out and locking functions. This is the operating system default screen.
Apps	The Apps screen contains shortcuts to the applications and utilities installed on the server. The server applications and utilities are grouped into categories. Third-party vendors and applications can also add custom, vendor or product specific, categories to the Apps screen.
Desktop	The Desktop screen contains the Windows start button, the Windows Taskbar, Recycle Bin, and shortcuts to the Windows Explorer utility, among others. The Taskbar displays the Windows Notification Area and System Tray. The notification area is located on the right portion of the Taskbar next to the time.

Navigation tips:

- Use the up  and down  arrow icons to navigate between the **Start** and **Apps** screens.
- To display the **Start** screen, on the **Desktop** screen, click the Windows start button.
- To display the **Desktop** screen, on the **Start** screen select the **Desktop** tile.
- To display the **Desktop** screen, on the **Apps** screen select the **Desktop** tile.
- To switch between the **Start** screen and the **Desktop** screen press the Windows start button on your keyboard.
- To access the Control Panel, on the **Apps** or **Start** screen click on the **Control Panel** tile.
- To access the Administration Tools, on the **Apps** or **Start** screen click on the **Administrative Tools** tile.

These screen navigation methods work when you are using the server's keyboard and mouse directly, or when you are using Remote Desktop to access the server.

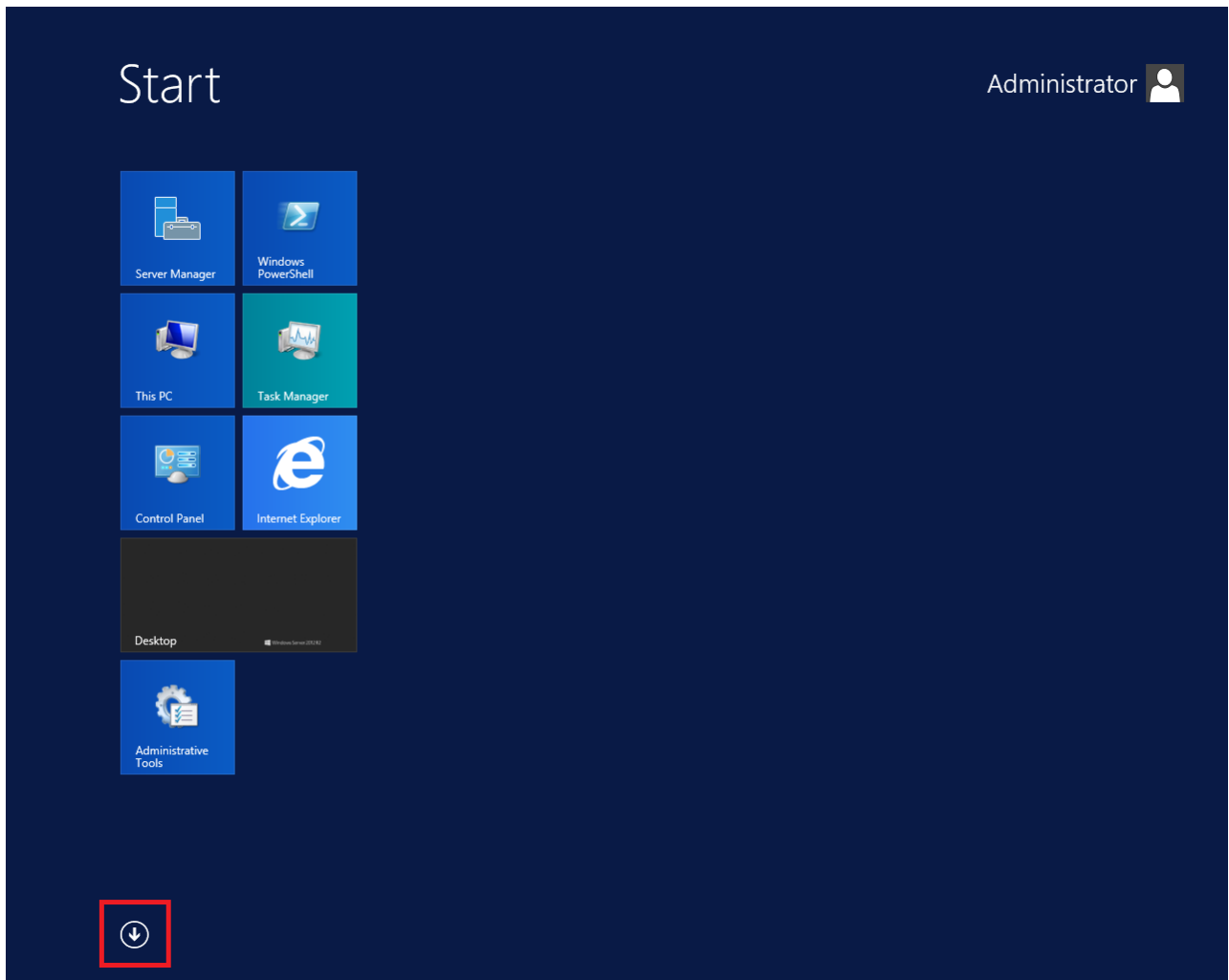


Figure 4: Example of the Start screen, with the down arrow icon highlighted in a red box.

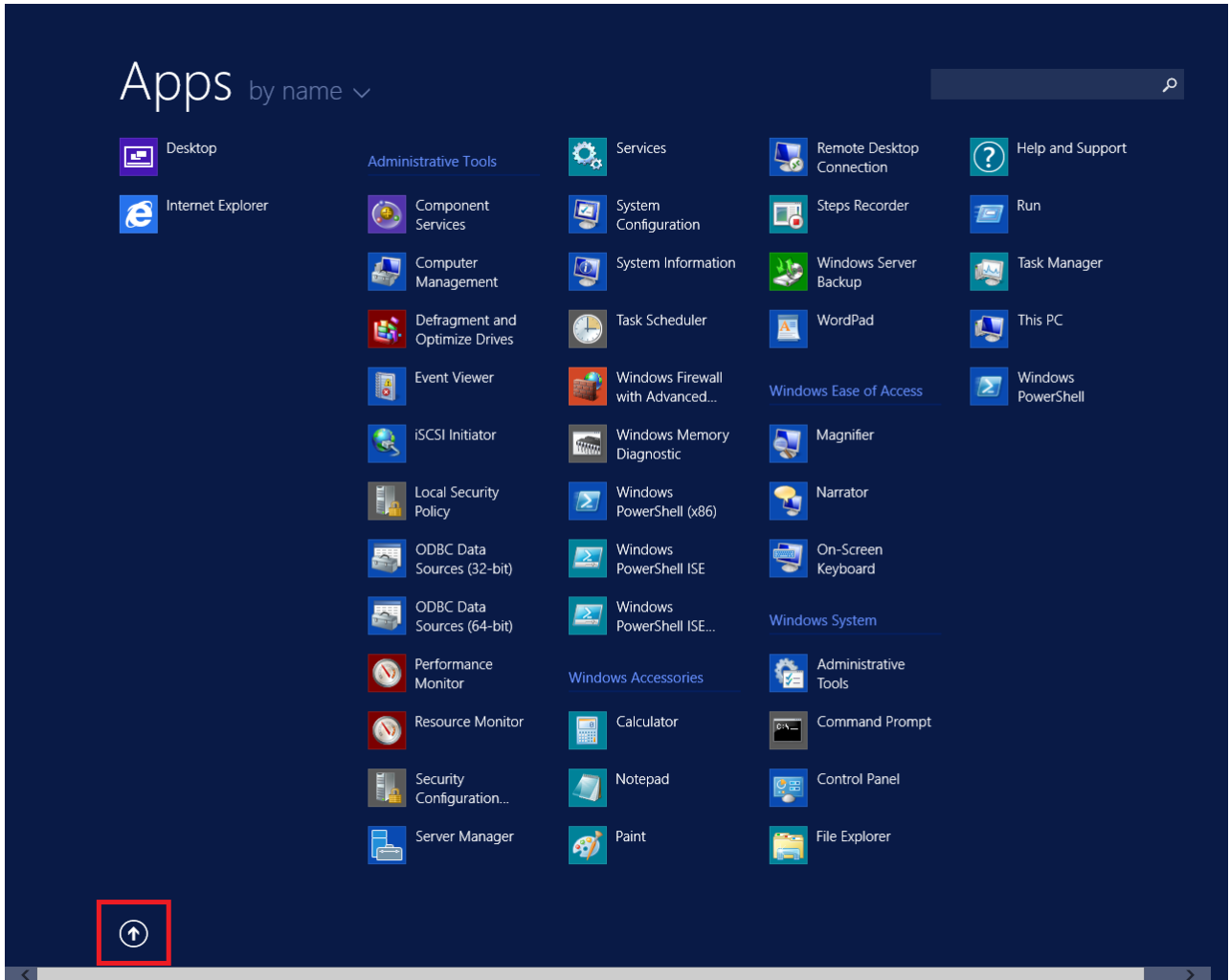


Figure 5: Example of the Apps screen, with the up arrow icon highlighted in a red box.

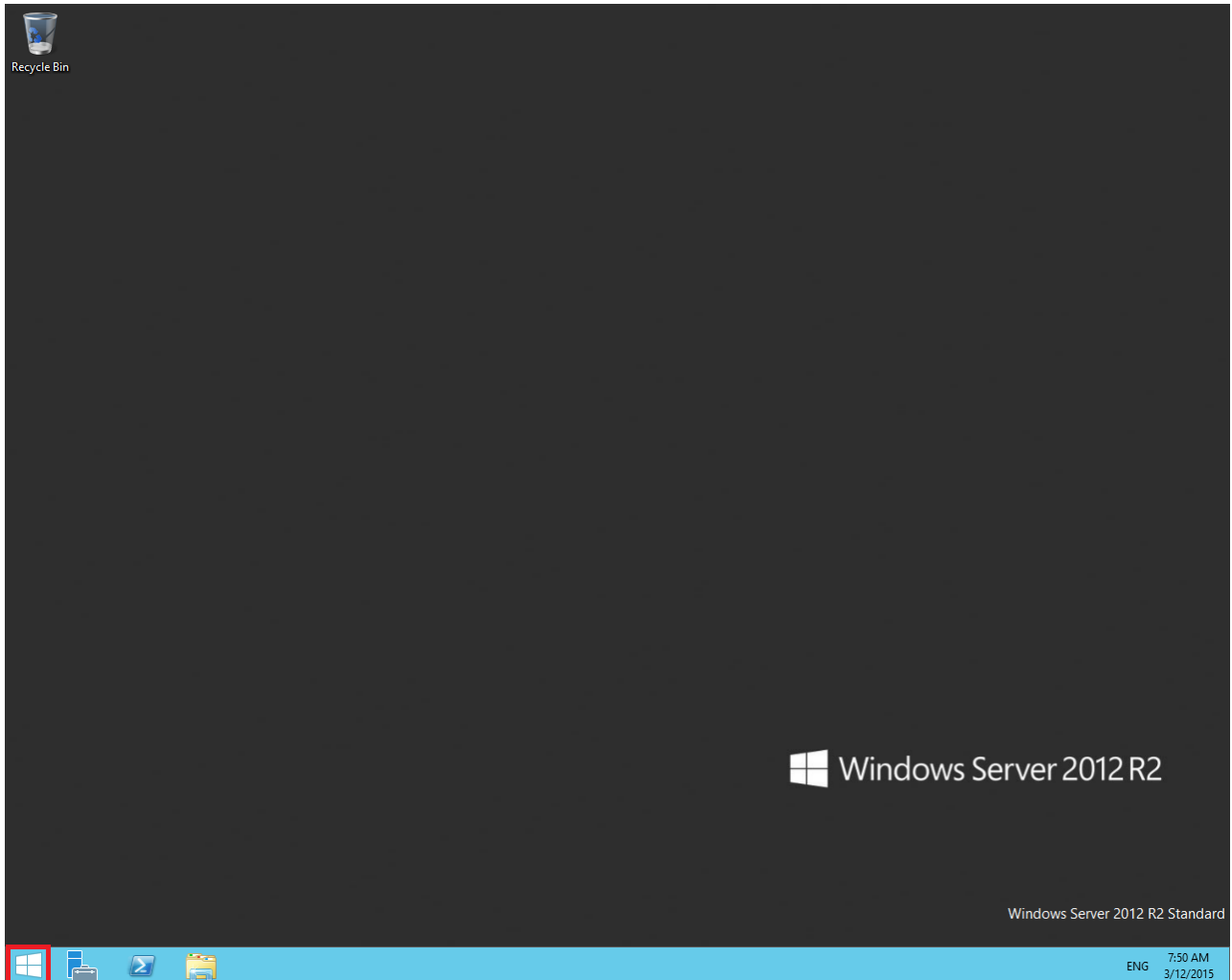






Figure 6: Example of the Desktop screen, with the Windows start button highlighted in a red box.

The following table describes some of the Taskbar sections of the **Desktop** screen.

Icon	Name	Description
	Windows start button	Use the Windows start button to navigate to the Start screen. Use this button to switch between the Start screen and the Desktop screen.
	Server Manager	Use this button to access the Server Manager to configure the roles and features to the server.
	PowerShell	Use the PowerShell button to start the Windows PowerShell console. Windows PowerShell is a command-line shell that provides cmdlets (pronounced command-lets) for server configuration and management. PowerShell also provides scripting functions for task automation.
	This PC	Use this button to start the This PC Windows Explorer. Use this to access and navigate the folders, files, and storage devices on the server.

The contents of your screens can vary depending on the roles, features, and applications installed on your server.

For more information about the Windows Server 2012 R2 operating system, refer to the Microsoft support website and Microsoft product documentation.

Installing Microsoft Windows Server 2016 or Windows Server 2019

Before you begin

- Ensure that you have a newly formatted server that meets the specifications in *Avaya Contact Center Select Solution Description* on which to install Microsoft Windows Server 2016 or Windows Server 2019.

Do not upgrade your operating system from a previous release. Contact Center is not supported on an upgraded operating system.

- Configure all servers for RAID as described in *Avaya Contact Center Select Solution Description*.
- Ensure that you have a DVD for Microsoft Windows Server 2016 or Windows Server 2019 *Standard* or *Data Center*.
- Ensure that you have a Microsoft Windows Server 2016 or Windows Server 2019 operating system product key.
- Know the IP addresses for the contact center subnet.

About this task

Install the Microsoft Windows Server 2016 or Windows Server 2019 *Standard* or *Data Center* operating system and configure it to support Contact Center server software.

The following table lists the main inputs to consider while installing the operating system.

Name	Description
Computer name	Do not use spaces or underscores or exceed 15 characters. The name must start with an alphabetic character. Server names must adhere to RFC1123. Avaya recommends that you configure the server final production name before installing Contact Center software. The computer name must match (including case sensitivity) the DNS name.
Disk drives	Format the partitions as required for the server. For more information, see <i>Avaya Contact Center Select Solution Description</i> .
Domain name	Configure as required for your site. You must check to ensure the DNS Domain name (including case) matches the server name if the server is added to a domain after configuration.

Table continues...

Name	Description
Licensing modes	Select Per server licensing mode. Accept the default five concurrent connections.
Network components	Configure IP Address, WINS, DNS for one or two network cards as per configuration. Contact Center does not support IPv6.
Network connections	If the server has more than one NIC/adaptor, ensure contact center subnet appears first in the network adapter binding order.
Hard Disk Partitions	Configure C: drive to be a primary drive. Configure the other drives on your server to meet the requirements according to <i>Avaya Aura® Contact Center Overview and Specification</i> for the server.

Perform this procedure on each server before you install Contact Center server software on the server.

Procedure

1. Insert the Microsoft Windows Server 2016 or Windows Server 2019 *Standard* or *Data Center* DVD into the DVD drive.
2. Turn on the power to the server.
The server begins to boot up.
3. On the **Windows Setup** screen, select a **Language to install** from the list.
4. Select a **Time and currency format** from the list.
5. Select **Keyboard or input method** from the list.
6. Click **Next**.
7. Click **Install now**.
8. On the **Activate Windows** window, enter the operating system product key.
9. Click **Next**.
10. On the **Windows Setup** screen, select a version of Windows Server 2016 or Windows Server 2019 *Standard* or *Data Center* that includes a Graphical User Interface (GUI). Install a version that includes "**Desktop Experience**".
11. Click **Next**.
12. On the **Windows Setup** screen, read the terms of the license agreement and select **I accept the license terms**.
13. Click **Next**.
14. Select **Custom: Install Windows only (advanced)** to install a clean new installation of the operating system.
15. Select the disk partition on which you want to install Windows Server 2016 or Windows Server 2019.

 **Important:**

You can use the partition management options to configure the partitions on your server.

16. Click **Next**.

The installation proceeds and automatically restarts the server several times.

17. After completing the installation, log in to the server as Administrator.

You must enter and confirm the Administrator password.

18. After logging in, configure the time zone settings for your server.

19. Specify the server IP address for your Network Interface Card (NIC).

20. Configure your computer name and domain.

21. **(Optional)** Change the DVD drive letter to E: to ensure the correct drive letters are free for the Contact Center application and database hard disk drives and partitions.

22. Configure the hard disk drives and partitions for this server using the Windows Server 2016 or Windows Server 2019 Computer Management - Disk Management utility. For more information about hard disk drives and partitions, see *Avaya Aura® Contact Center Overview and Specification*.

23. Install other required drivers for your hardware configuration.

Contact Center virtual machine hard disks and partitions

Create individual virtual hard disks for each of the required partitions for your Contact Center virtual machine. When creating a virtual hard disk for the Operating System partition, create a hard disk size 1GB greater than the required partition size to accommodate the creation of any additional Windows partitions which might be created automatically as part of the Windows Server install.

For example, for an Operating System partition size requirement of 80GB, create an 81GB virtual hard drive. For each additional Contact Center required partition, create a virtual hard drive greater than or equal to the partition size requirement. The virtual hard disk must be of sufficient size such that when the associated partition is created and formatted it has a size matching the required partition size for the install.

For improved multimedia offline data retention, Avaya recommends using a 600 GB partition for multimedia storage. The multimedia 600 GB partition requires SAN Storage.

Table 2: Contact Center Virtual Machine hard disk minimum partition sizes

Hard disk drive partition description	Drive letter	Minimum partition sizes	Recommended partition sizes, 300 GB multimedia partition	Recommended partition sizes, 600 GB multimedia partition
Operating System drive	C:	80 GB NTFS partition	80 GB NTFS partition	80 GB NTFS partition
Application drive	D:	100 GB NTFS partition	120 GB NTFS partition	120 GB NTFS partition
DVD drive	E:	—	—	—
Voice Contact Server database drive	F:	180 GB NTFS partition	200 GB NTFS partition	200 GB NTFS partition
Multimedia Contact Server database drive	G:	200 GB NTFS partition	300 GB NTFS partition	600 GB NTFS partition
Database journal drive	H:	80 GB NTFS partition	100 GB NTFS partition	100 GB NTFS partition
	Total	641 GB of Thick Provisioned disk space in a VMware datastore.	801 GB of Thick Provisioned disk space in a VMware datastore.	1101 GB of Thick Provisioned disk space in a SAN datastore.

If using 900 GB Raid–1 disks, use the above Minimum Partition size option.

Contact Center requires Hardware RAID-1 with duplicate hard disk drives with identical specifications. Therefore, the VMware host server must implement Hardware RAID-1 or better.

Navigating the Microsoft Windows Server 2016 or Windows Server 2019 User Interface

This section describes how to navigate the main user interface screens of the Windows Server 2016 and Windows Server 2019 operating system.

The following table describes some of the main Microsoft Windows Server 2016 and Windows Server 2019 user interface items, and compares them with the corresponding items on the Windows Server 2012 R2 user interface.

User interface item	Description
Start button	The Start button opens a list of shortcuts to the main administration interfaces of the server, including shortcuts to Contact Center applications. The Start button displays the currently logged on user and provides some basic server log out and locking functions. The Start button offers similar functionality as the Windows Server 2012 R2 Start screen and App screen.
Desktop screen	The Desktop screen contains the Windows start button, the Windows Taskbar, Recycle Bin, and shortcuts to the Windows Explorer utility, among others. The Taskbar displays the Windows Notification Area and System Tray. The notification area is located on the right portion of the Taskbar next to the time. The Desktop screen is the same on Windows Server 2019, Windows Server 2016, and Windows Server 2012 R2.

Navigation tips:

- To display the **Start** menu, on the **Desktop** screen, click the Windows start button.
- To access the Control Panel, on the **Start** menu click on the **Control Panel** tile.
- To access the Administration Tools, on the **Start** menu click on the **Windows Administrative Tools** tile.

The contents of your screens can vary depending on the roles, features, and applications installed on your server.

For more information about the Windows Server 2016 or Windows Server 2019 operating system, refer to the Microsoft support website and Microsoft product documentation.

 **Important:**

Contact Center documentation describes how to perform all procedures using Windows Server 2012 R2 only. Use this section to determine how to perform the same procedures on a Windows Server 2016 or Windows Server 2019 operating system.

Installing the most recent supported operating system service packs

Before you begin

- Access the Avaya hotfixes list on the website <http://support.avaya.com>.
- Review the specifications on operating system service updates in *Avaya Contact Center Select Solution Description*.

About this task

Avaya recommends that you install the most recent supported operating system service packs. You must download the supported operating system service pack from the Avaya hotfixes list to ensure your Contact Center server software functions correctly with the supported operating system patches.

Procedure

1. Review the Contact Center Service Packs Compatibility and Security Hotfixes Applicability List to determine the most recent Contact Center supported patches or service packs.
2. Download the appropriate Microsoft Windows Server patches for the Contact Center software installed on this server.
3. Install the most recent Microsoft Windows Server service pack that is validated with Contact Center by following the Microsoft Installation instructions.

Installing VMware Tools

About this task

Install VMware Tools on the Contact Center virtual machine. VMware Tools provides performance monitoring, networking drivers, and improved mouse performance.

Procedure

1. Using VMware vSphere client, in the left pane, right-click on the Contact Center virtual machine and select **Guest > Install/Upgrade VMware Tools**.
2. Follow the on-screen instructions.
3. To complete installing VMware Tools, reboot the virtual machine.

Connecting to the contact center subnet

About this task

Connect the Contact Center server to the contact center subnet. The contact center subnet is the network on which the server software applications work together to route contacts and generate reports.

Procedure

1. Locate the slot assigned to the contact center subnet network interface card for the server. Make a note of the slot.
2. Connect the cable from the contact center subnet to the contact center subnet network interface card in the server in accordance with customer site networking guidelines.
3. Use the ping command to test the contact center subnet.

Connecting the server to the network

About this task

Connect the Contact Center server to the local contact center subnet. Disable all unused Network Adapters or Network Interface Cards (NICs) to improve network communications and prevent the erroneous configuration of unused NICs during Contact Center server commissioning.

Ask your System Administrator to add a Domain Name System (DNS) static entry for this server. Each Contact Center server in a domain requires a DNS static entry.

Procedure

1. Using a network cable, connect the Contact Center server to the contact center subnet. The contact center subnet is the network on which the server software applications work together to route contacts and generate reports. Use the ping command to test the contact center subnet connection.
2. Log on to the server.
3. On the **Start** screen, click **Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings**.
4. Right-click on the unused Network Adapter, and select **Disable**.
5. Repeat this procedure for all unused Network Adapters.

Downloading the most recent Contact Center patches to the server

Before you begin

- Download and install the most recent and supported updates for Microsoft Windows Server.
- Know the location at which you plan to install each Contact Center server software package.
- Ensure that you use one administrator account on your server to un-install and install software updates.

About this task

To ensure that you have the most current software, download the most recent Contact Center patches from <http://support.avaya.com> to the server you plan to install.

Procedure

1. Log on to the server using the administrator account.
2. Create a folder <Drive>:\Avaya-ProductUpdates\ to save the software updates. Where <Drive> is the drive letter on which you want to save the Contact Center software updates.
3. Download the most recent service pack file. Save and unzip the file on the Contact Center server in the Avaya-ProductUpdates folder.

4. If new patches are available for the latest service pack, download and save the patches on the Contact Center server in the Avaya-ProductUpdates folder.
5. Read the Contact Center Release Notes for the most recent instructions.

Enabling Microsoft Remote Desktop connection

About this task

Enable Microsoft Remote Desktop connection as your remote access tool. Microsoft Remote Desktop provides remote access for support on the server.

Procedure

1. Log on to the server with administrator privileges.
2. On the **Start** screen, select **Control Panel** > **System and Security**.
3. In the **System** section, select **Allow remote access**.
4. Click the **Remote** tab.
5. Select **Allow remote connections to this computer**.
6. Click **Apply**.
7. Click **OK**.

Disabling Admin Approval Mode for Windows Server administrators

About this task

Windows Server implements a security feature known as User Account Control (UAC). By default, this feature causes applications run by local non built-in administrators to behave as if the applications had been run by standard users. Perform this procedure to ensure that local administrators get full privileges for running applications.

Note:

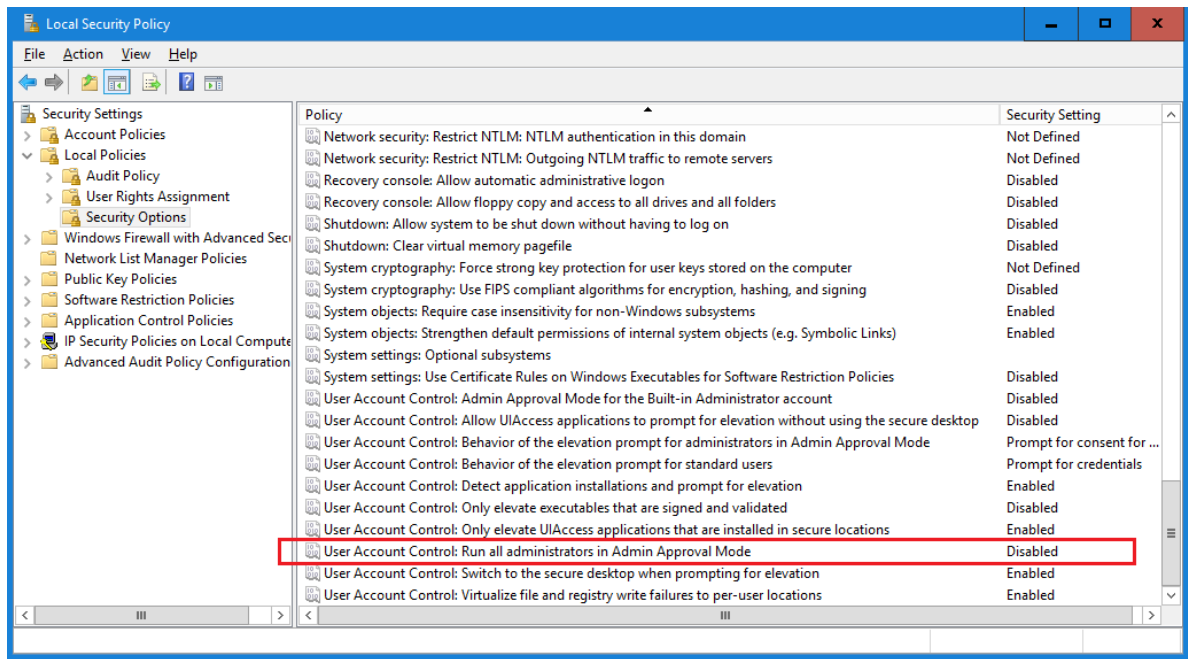
This procedure describes how to disable Admin Approval Mode on the Contact Center server using one method only; there are additional methods available. For example, you can also administer User Account Control settings for the Contact Center server using a group policy.

Procedure

1. On the **Start** screen, select **Administrative Tools** > **Local Security Policy**.
2. Under **Security Settings**, expand **Local Policies**.

3. Select **Security Options**.
4. In the policy pane on the right, double-click on **User Account Control: Run all administrators in Admin Approval Mode**.
5. Click the **Local Security Setting** tab, and select **Disabled**.
6. Click **OK**.

If prompted, restart the server.



Creating a shared location for security configuration

About this task

If you want to enable security on the Contact Center server, and complete security configuration when installing Contact Center software, you must ensure that a shared network location exists on the Contact Center server. You can then export the Certificate Signing Request (CSR) file to this location using the Contact Center Ignition Wizard.

Procedure

Create a shared network location on the Contact Center server.

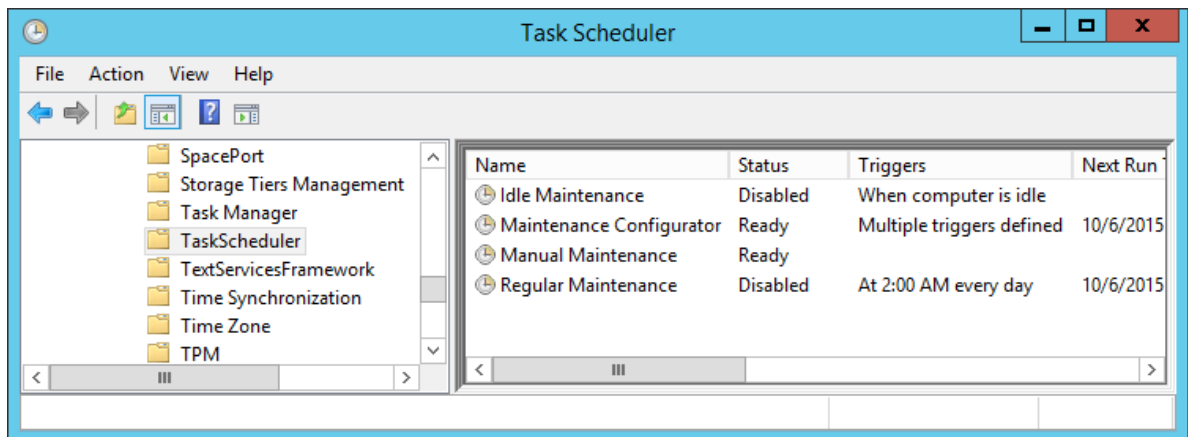
Disabling Windows Server Automatic Maintenance

About this task

Disable Windows Server Automatic Maintenance while installing Contact Center software. Windows Server Automatic Maintenance can occasionally interfere with the real-time requirements for Contact Center deployment and configuration. You must therefore temporarily disable Automatic Maintenance to install and configure Contact Center software. You re-enable Automatic Maintenance after deploying and configuring Contact Center.

Procedure

1. Log on to the Contact Center server as Administrator.
2. On the **Desktop** screen, right-click **Start** and select **Run**.
3. In the **Run** text box, type `Taskschd.msc`.
4. Click **OK**.
5. On the **Task Scheduler** window, in the left pane, select **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
6. In the **Name** column, right-click **Idle Maintenance** and select **Disable**.
7. In the **Name** column, right-click **Regular Maintenance** and select **Disable**.



8. From the **File** menu, select **Exit**.

Installing Avaya Contact Center Select without Avaya Aura[®] Media Server Release 7.1 DVD software

Before you begin

- Download the most recent Avaya Contact Center Select patches to the server.

- Download the most recent Avaya Contact Center Select Release Notes.
- If you want to install Avaya Workspaces, you must manually deploy three virtual machines using the Avaya Workspaces Open Virtual Appliance (OVA). See [Deploying the Avaya Workspaces OVA](#) on page 156.

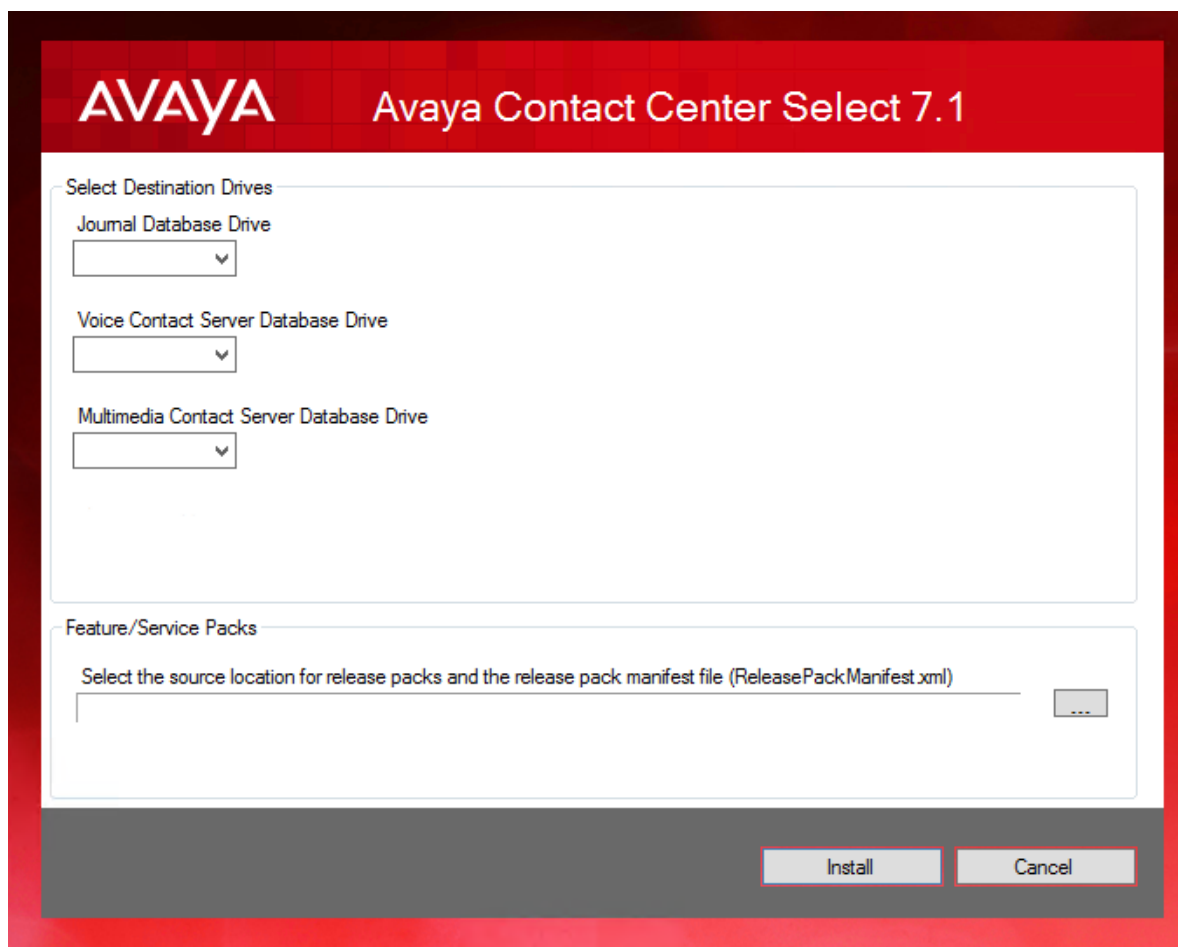
About this task

Install the Avaya Contact Center Select without Avaya Aura® Media Server software and enable your contact center to route contacts to the agents.

Procedure

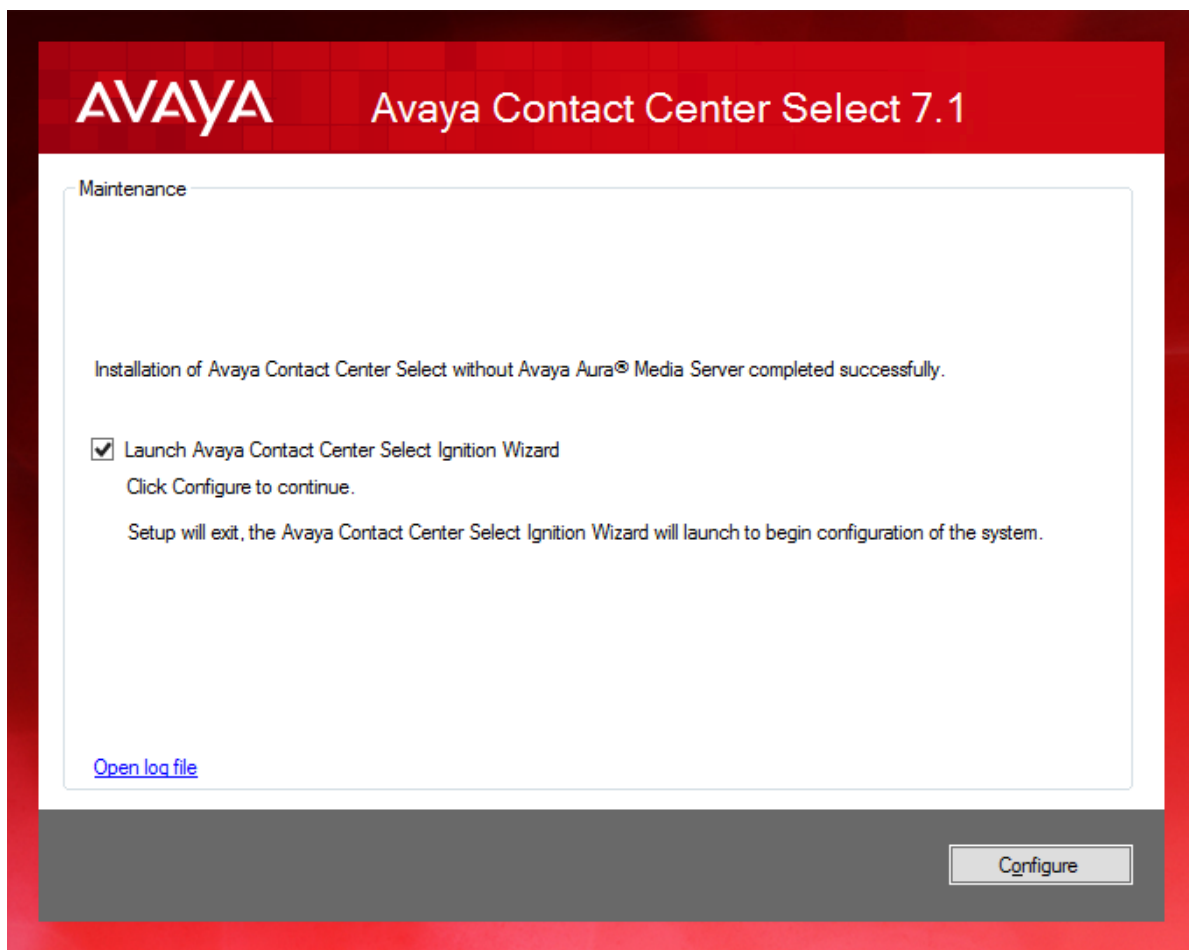
1. Read the Avaya Contact Center Select Release Notes for the most recent instructions.
2. Mount the Avaya Contact Center Select DVD or ISO file in your virtual environment so that it is available on the virtual guest as a DVD drive.
3. Double click the DVD drive on the virtual server.
If the installation does not automatically start, access the DVD drive and double-click **Setup.exe**.
4. Click **Install** to install the necessary software libraries on the server.
If you are prompted to accept the Microsoft .NET Framework license agreement, click **Accept**. If you are prompted to restart the server, click **Yes**.
5. After the prerequisite software and libraries are installed, navigate to the Avaya Contact Center Select DVD and double-click **Setup.exe** to install the application software.
6. The Avaya Contact Center Select installer starts and verifies that the server meets the minimum hardware and Operating System requirements:
 - If the system checker detects server errors, it displays a **System information** window listing the detected blocking issues. Review the displayed issues, click **Cancel**, and consult *Avaya Contact Center Select Solution Description* to determine the actions to resolve the issue.
 - If the system checker detects non-blocking warnings, it displays a **System information** window listing the detected issues. Review the displayed issues and consult *Avaya Contact Center Select Solution Description* to determine the actions to resolve the issue. You can ignore warnings if the potential impact to the operation of the contact center is understood and not applicable. Click **Ignore** or **Cancel**.
 - If the system checker does not detect issues, the **System information** window is not displayed.
7. On the **Select Deployment Type** screen, select **Avaya Contact Center Select without Avaya Aura® Media Server**.
8. **(Optional)** If you want to install and configure Avaya Workspaces, select the **Configure Workspaces** check box.
9. Click **Next**.

10. The **Select Destination Drive** window appears.



11. From the **Journal Database Drives** list, select the drive for the database journal file.
12. From the **Voice Contact Server Database Drive** list, select the drive for the voice databases.
13. From the **Multimedia Contact Server Database Drive** list, select the drive for the Contact Center Multimedia database.
14. In the **Service Packs** section, browse to locate the folder containing the Avaya Contact Center Select product updates.
15. Click **Install**.
16. The **AVAYA GLOBAL SOFTWARE LICENSE TERMS** window appears.
17. Read the terms of the license.
 - If you accept the terms, click **I ACCEPT THE LICENSE TERMS**. *The installation continues.*
 - If you do not accept the terms, click **I DECLINE THE LICENSE TERMS**. *The installation returns to the Select Destination Drive screen.* Click **Cancel** to stop the install.

- To print the license terms, click **Print**.
18. The **MICROSOFT SOFTWARE LICENSE TERMS** window appears.
 19. Read the terms of the license.
 - If you accept the terms, click **I ACCEPT THE LICENSE TERMS**. *The installation continues.*
 - If you do not accept the terms, click **I DECLINE THE LICENSE TERMS**. *The installation returns to the Select Destination Drive screen.* Click **Cancel** to stop the install.
 - To print the license terms, click **Print**.
 20. The **Progress** window appears and displays the installation progress.
 21. After a successful installation, the following window appears.



22. When the software is installed, you have the following options.
 - To continue configuring the server installation data:
 - a. Select the **Launch Avaya Contact Center Select Ignition Wizard** check box.
 - b. Click **Configure**. This starts the Avaya Contact Center Select Ignition Wizard.

- To defer configuring the server installation data:
 - a. Clear the **Launch Avaya Contact Center Select Ignition Wizard** check box.
 - b. On the message box, click **Yes**.
 - c. On the main installer screen, click **Close**.
 - d. Follow the on-screen instructions and shut down the Avaya Contact Center Select server.

You must use the Ignition Wizard to initialize Avaya Contact Center Select, otherwise Avaya Contact Center Select is not operational. For more information about the Ignition Wizard, see the following procedures.

Next steps

Use the Ignition Wizard to configure Avaya Contact Center Select.

Configuring the server installation data

Before you begin

- Know the IP address of the IP Office primary call server.
- Know the IP Office Service User account name and password.
- Know the IP Office System Password. Ask your IP Office Administrator for the System Password.
- Configure an IP Office SIP User Extension Number to be used to register Avaya Contact Center Select.
- Configure an IP Office short code to forward customer calls to an Avaya Contact Center Select CDN (Route Point).
- Install an Avaya WebLM server. Know the IP address and port number of the Avaya WebLM server.
- Install an Avaya Aura[®] Media Server server. Know the IP address and port number of the Avaya Aura[®] Media Server server.
- If your Avaya Contact Center Select solution is going to support email contacts, configure the mailbox details on your email server that you use to receive inbound email messages intended for the Avaya Contact Center Select. Know the name and password for this mailbox.
- If your Avaya Contact Center Select solution is going to support email contacts, know the host name of your email host server.
- You must configure the required language and locale of the Contact Center server operating system, if it is not a Latin-1 language, before configuring the Contact Center server using the Contact Center Ignition Wizard. For more information about configuring language and locale settings on the Contact Center server, see *Avaya Contact Center Select Advanced Administration*.

About this task

Configure the Avaya Contact Center Select installation data to enable communication with an IP Office primary call server.

Optionally, if your solution is to support routed email contacts, configure the mailbox details on your email server that you use to receive inbound email messages intended for the Avaya Contact Center Select. Avaya Contact Center Select logs onto this mailbox on your mail server and retrieves email at defined intervals. Email messages are then routed to agents. To route an email, Avaya Contact Center Select requires the mailbox name and password.

Procedure

1. Select the Avaya Contact Center Select virtual machine from the list of virtual machine on the target VMware host.
2. With the Avaya Contact Center Select virtual machine still selected, right-click the mouse and select **Open Console**.
3. In the Avaya Contact Center Select console, log on to the Avaya Contact Center Select virtual machine using the Administrator account details.
4. The Avaya Contact Center Select **Welcome** screen appears.



5. Click **Next**.

6. On the license screen, select **I Accept the Terms of the End-User License Agreement**.
7. Click **Next**.

Avaya Contact Center

Configuration Data

Enter the required configuration data.

IP Office
 Sample Data
 Core
 Licensing
 Multimedia
 Security Configuration

IP Office Server

IP Address:

Voice Port:

Transport:

IP Office SIP Domain Name:

IP Office Service User

Username:

Password:

Confirm Password:

IP Office SIP Extension

Extension Number:

Password:

Confirm Password:

The Contact Center application registers to the IP Office as this SIP extension number.

This SIP extension number must be manually created on the IP Office.

IP Office System Password

Password:

Confirm Password:

Click Next to Continue

8. On the **Configuration Data** screen, select the **IP Office** tab.
9. In the **IP Office Server** section, in the **IP Address** box, type the IP address of the IP Office primary call server.
10. In the **Voice Port** box, type the port number of the IP Office primary call server. The default port number is 5060.
11. From the **Transport** list, select the network transport communication protocol for the IP Office primary call server. The default protocol is TCP.
12. In the **IP Office SIP Domain Name** box, type the SIP domain name of your IP Office primary call server. The Avaya Contact Center Select SIP domain name must match your IP Office SIP domain name.
13. In the **IP Office SIP Extension** section, in the **Extension Number** box, type the IP Office SIP User Extension Number used to register Avaya Contact Center Select. For more information, see [Configuring the SIP User Extension Number](#) on page 42.
14. In the **IP Office SIP Extension** section, in the **Password** box, type the password of the IP Office SIP User Extension Number used to register Avaya Contact Center Select. Enter the number that you configured for the Supervisor Settings - Login Code on the user's

Telephony tab. For more information, see [Configuring the SIP User Extension Number](#) on page 42.

15. In the **IP Office SIP Extension** section, in the **Confirm Password** box, re-type the password.
16. In the **IP Office Service User** section, in the **Username** box, type the name of your IP Office data synchronization service user. For more information, see [Configuring an IP Office service user for data synchronization](#) on page 37.
17. In the **IP Office Service User** section, in the **Password** box, type the password of your IP Office data synchronization service user.
18. In the **IP Office Service User** section, in the **Confirm Password** box, re-type the password.
19. In the **IP Office System Password** section, in the **Password** box, type the *System Password* for your IP Office call server. Ask your IP Office Administrator for the System Password.
20. In the **IP Office System Password** section, in the **Confirm Password** box, re-type the *System Password* for your IP Office call server.
21. Select the **Sample Data** tab.

The screenshot shows the 'Configuration Data' interface for Avaya Contact Center. The 'Sample Data' tab is selected. The interface includes the following elements:

- Avaya Contact Center** header at the top.
- Configuration Data** title and the **AVAYA** logo.
- Instruction: "Enter the required configuration data."
- Navigation tabs: IP Office, **Sample Data**, Core, Licensing, Multimedia, Security Configuration.
- Contact Center Sample Data** section with four input fields:
 - Sample Agent Starting ID: 6001
 - Sample Agents Templated: 10
 - Sample CDN (Route Point): 3000
 - Callback Mailbox Number: 6999
- Sample Agent's Password** section with instructions: "Enter a password for the Contact Center Sample Agents Windows accounts." and two input fields for Password and Confirm Password.
- Footer: "Click Next to Continue" and navigation buttons: < Back, Next >, Cancel.

22. In the **Contact Center Sample Data** section, in the **Sample Agent Starting ID** box, type a phone number for the first sample Avaya Contact Center Select agent. Avaya Contact Center Select automatically creates ten sample agents, using this number as the first of ten sequential agent numbers. The default number is 6001.
23. In the **Sample CDN (Route Point)** box, type a number for the Avaya Contact Center Select CDN (Route Point). This number must match an IP Office short code entry number. For more information, see [Configuring a shortcode to Contact Center Route Points](#) on page 42. The default number is 3000.
24. In the **Callback Mailbox Number** box, type the voice mail mailbox number. This voice mail number is used by the Customer Service sample application in Orchestration Designer. The default number is 6999.
25. In the **Sample Agent's Password** section, in the **Password** box, type a password for the Windows accounts of the sample agents. Avaya recommends that you enter a password that conforms to your corporate password policy.
26. In the **Confirm Password** box, re-type the password for the Windows accounts of the sample agents.
27. Select the **Core** tab.

The screenshot shows the 'Avaya Contact Center Configuration Data' window. The 'Core' tab is selected. The 'Avaya Aura® Media Server' section contains fields for IP Address, Port (5060), and IP Office Contact Center Media Services Locale (en_us). The 'System Account Configuration' section contains fields for Password and Confirm Password. The Avaya logo is visible in the top right corner. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

28. In the **Avaya Aura® Media Server** section, in the **IP Address** box, type the IP address of your Avaya Aura® Media Server.

29. In the **Port** box, type the port number for your Avaya Aura® Media Server. The default port number is 5060.
30. From the **IP Office Contact Center Media Services Locale** list, select the locale (including language and dialects) of the solution environment.
31. In the **System Account Configuration** section, in the **Password** box, type a password for the Avaya Contact Center Select administration account. The password is not checked against the server security policy for minimum password requirements. Avaya recommends that you enter a password that conforms to your corporate password policy.
32. In the **Confirm Password** box, type the password.
33. Select the **Licensing** tab.

The screenshot shows the 'Configuration Data' screen for Avaya Contact Center. The title bar reads 'Avaya Contact Center'. The main heading is 'Configuration Data' with the AVAYA logo to the right. Below the heading is the instruction 'Enter the required configuration data.' There are several tabs: 'IP Office', 'Sample Data', 'Core', 'Licensing' (which is selected), 'Multimedia', and 'Security Configuration'. Under the 'Licensing' tab, there are two main sections. The first is 'License Type' with a dropdown menu showing 'Remote WebLM'. The second is 'Remote Avaya WebLM Server' with two sub-fields: 'IP Address' (empty) and 'Port' (containing '52233'). At the bottom left, it says 'Click Next to Continue'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

34. From the **License Type** list, select **Remote WebLM**.
35. In the **IP Address** box, type the IP address of the remote Avaya WebLM server.
36. **(Optional)** To configure the Avaya WebLM centralized licensing, select the **Centralized** check box and, in the **CLID** box, type the Centralized License ID (CLID) of the ACCS server.
37. Select the **Multimedia** tab.

Avaya Contact Center

Configuration Data

Enter the required configuration data.

AVAYA

IP Office
Sample Data
Core
Licensing
Multimedia
Security Configuration

Mailbox Configuration

Mail Provider

Display Name

Email

Password

Confirm Password

Incoming Mail Server

Host Name

Protocol

Encryption

Port

Outgoing Mail Server

Host Name

Protocol

Encryption

Port

SMTP Authentication

Click Next to Continue

38. In the **Mailbox Configuration** section, from the **Mail Provider** list, select None, Microsoft Exchange, Gmail, Outlook Hotmail, Yahoo, or Other (POP3/IMAP). The default is Microsoft Exchange. If Avaya Contact Center Select is not going to process email contacts, select **None**. If you select Gmail, Outlook Hotmail, or Yahoo, the Incoming Mail Server and Outgoing Mail Server sections are automatically populated for you.
39. In the **Mailbox Configuration** section, in the **Display Name** box, type a display name for the mailbox.
40. In the **Mailbox Configuration** section, in the **Email** box, type the email address for the mailbox. For example, sales@company.com.
41. In the **Mailbox Configuration** section, in the **Password** box, type the password for the mailbox.
42. In the **Mailbox Configuration** section, in the **Confirm Password** box, re-type the password for the mailbox.
43. In the **Incoming Mail Server** section, in the **Host Name** box, type the name of the server on which email messages are received in your network.
44. In the **Incoming Mail Server** section, from the **Protocol** list, select the communication protocol for the inbound email server. Select **POP3** or **IMAP**. The default protocol is POP3.

45. In the **Incoming Mail Server** section, from the **Encryption** list, select the encryption type to use. Select **Cleartext**, **TLS**, or **STARTTLS**.
46. In the **Incoming Mail Server** section, in the **Port** box, type the port number of the incoming email server. For the POP3 protocol, the default port number is 110. For the IMAP protocol, the default port number is 143.
47. In the **Outgoing Mail Server** section, in the **Host Name** box, type the name of the server from which email messages are sent. Your inbound and outbound mail servers can have the same name.
48. For outgoing email, the **Protocol** is SMTP.
49. In the **Outgoing Mail Server** section, from the **Encryption** list, select the encryption type to use. Select **Cleartext**, **TLS**, or **STARTTLS**.
50. In the **Outgoing Mail Server** section, in the **Port** box, type the port number of the outgoing email server. The default port number is 25.
51. In the **Outgoing Mail Server** section, from the **SMTP Authentication** list, select SMTP Authentication Disabled or Base 64 Encoded Authentication. The default authentication method is Base 64 Encoded Authentication.
52. **(Optional)** Select the **Workspaces** tab to configure optional Avaya Workspaces. See [Configuring Avaya Workspaces during the initial installation](#) on page 158 for the configuration details.
53. Select the **Security Configuration** tab, and configure the security details in the **Security Store Details** section.

The screenshot shows the 'Configuration Data' screen for Avaya Contact Center, specifically the 'Security Configuration' tab. The page title is 'Avaya Contact Center' and the main heading is 'Configuration Data'. The Avaya logo is in the top right. Below the heading, it says 'Enter the required configuration data.' There are several tabs: 'IP Office', 'Sample Data', 'Core', 'Licensing', 'Multimedia', and 'Security Configuration'. The 'Security Configuration' tab is active. It contains two main sections: 'Security Store Details' and 'Subject Alternative Name'. The 'Security Store Details' section has fields for 'Full Computer Name (FQDN)' (CC7SIP.aaccdomain.com), 'Encryption Algorithm Level' (SHA256), 'Key Size' (2048), 'Security Store Password', 'Confirm Store Password', 'Name of Organizational unit', 'Name of Organization', 'City or Locality', 'State or Province', and 'Two letter country code'. There is a 'Skip Security Configuration' checkbox. The 'Subject Alternative Name' section has a 'Type' dropdown (DNS) and a 'Value' input field. There are 'Add' and 'Remove' buttons. A 'Create Store' button is at the bottom right. At the bottom of the form, it says 'Click Next to Continue'. At the very bottom of the page, there are navigation buttons: '< Back', 'Next >', and 'Cancel'.

54. If you do not want to enable security, select the **Skip Security Configuration** checkbox and skip to [the next step](#) on page 144.

! **Important:**

A warning message appears. If you proceed without enabling security and IP Office is using TLS, you cannot test a first call quickly without additional configuration steps. The CTI link is disabled until you configure Contact Center TLS certificates to communicate securely with IP Office, or until you configure IP Office to allow an unsecured CTI connection. After the deployment, to complete your security configuration, follow the procedures in *Avaya Contact Center Select Advanced Administration*.

55. In the **Full Computer Name (FQDN)** box, type the full FQDN of the server on which you are creating the security store.

! **Important:**

The FQDN must be the full machine name of the server that the Security Store resides on. The FQDN name is case-sensitive.

56. In the **Name of Organizational unit** box, type the name of the department or division within the company.
57. In the **Name of Organization** box, type the company name.

58. In the **City or Locality** box, type the name of the city or district in which the contact center is located.
59. In the **State or Province** box, type the state or province in which the contact center is located.
60. In the **Two Letter Country Code** box, type the country code in which the contact center is located.
61. In the **Security Store password** box, type a password for accessing the new security store.
62. In the **Confirm Store password** box, confirm the password for accessing the new security store.

 **Important:**

Ensure you remember this password, because you need it when you log on to Security Manager after install. If you forget the password, you cannot access Security Manager.

63. If you are implementing High Availability in the contact center, generate the security store using Subject Alternative Names (SANs). In the **Subject Alternative Name** section, for each SAN you want to add:
 - a. From the **Type** drop-down list, select DNS.
 - b. In the **Value** field, type the FQDN for the server.
 - c. Click **Add**.

For a Business Continuity system, add the current server FQDN and the Managed name for the HA pair.

64. If you want to change the encryption setting, select the required encryption settings from the **Encryption Algorithm Level** and **Key Size** drop-down lists.

The default value for **Encryption Algorithm** is SHA256 and the default value for **Key Size** is 2048.

Contact Center displays a warning message if you select SHA1 or 1024. Contact Center includes these values for backward-compatibility only, because these settings do not meet the industry-recommended level of encryption.

65. Click **Create Store**.
66. You can now use the **Security Configuration** tab to create and save a Certificate Signing Request (CSR) file.

Avaya Contact Center

Configuration Data

AVAYA

Enter the required configuration data.

IP Office | Sample Data | Core | Licensing | Multimedia | Security Configuration

Store created – Generate Identity Security Certificate by signing the Certificate Signing Request provided.

Certificate Signing Request file

Create CSR File

Add

Imported Trusted Certificate Authority Root Certificate(s)

Remove

Imported Identity Security Certificate

Remove

Status

Ensure that a removable or network drive is available.

Create the Certificate Signing Request file and save it to a removable or network drive.

Alternatively, to defer Security Configuration and continue with the Installation Wizard.

Reset

Click Next to Continue

< Back | Next > | Cancel

67. Click **Create CSR File**.

68. From the **Save In** drop-down list, select a shared location in which to save the CSR file and click **Save**.

You must now send the Certificate Signing Request file to a Certificate Authority and receive a signed certificate and root certificate to import to the security store.

69. Click **Add** to import certificates. In the **Open** dialog box, navigate to the location of a certificate and click **Open**. To remove the imported certificate, select the required certificate from the list and click **Remove**.

You can import either a chained certificate, or separate root and signed certificates. Root certificates appear in the **Imported Trusted Certificate Authority Root Certificate(s)** section. A signed certificate appears in the **Imported Identity Security Certificate** section.

If a chained certificate contains both root and signed certificates, you can add root certificates and signed certificate simultaneously by importing just one chained certificate.

If a chained certificate contains root certificates only, you can use the chained certificate to add all root certificates at a time. To add a signed certificate, click **Add** and navigate to the required signed certificate.

If you have separate root and signed certificates, you must add them one by one by clicking the **Add** button. Always add a signed certificate last.

 **Important:**

When adding a chained certificate, the system can ask you to enter the password you created for accessing the security store. See [the previous steps](#) on page 142.

70. Click **Next**.

71. Review and confirm your inputs, and click **Configure**.

The configuration utility begins to configure the Avaya Contact Center Select components.

72. When the Avaya Contact Center Select is configuration details are applied, the **Configuration Complete** screen appears.

73. Click **Finish**.

74. On the **Avaya Contact Center** message box, click **OK** to restart Avaya Contact Center Select.

Avaya Contact Center Select software is now installed on the virtual machine.

Enabling Windows Server Automatic Maintenance

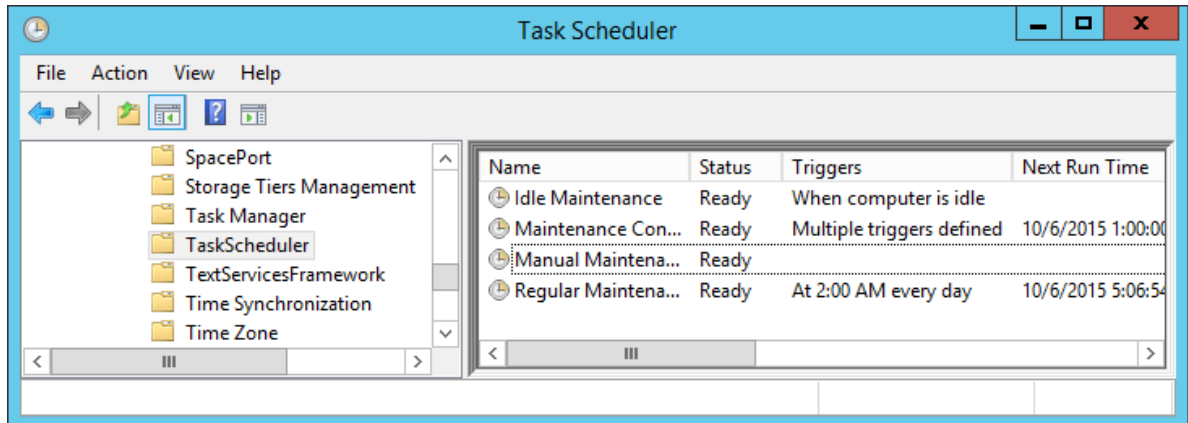
About this task

Enable Windows Server Automatic Maintenance after deploying and configuring Contact Center software.

Procedure

1. Log on to the Contact Center server as Administrator.
2. On the **Desktop** screen, right-click **Start** and select **Run**.
3. In the **Run** text box, type `Taskschd.msc`.
4. Click **OK**.
5. On the **Task Scheduler** window, in the left pane, select **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
6. In the **Name** column, right-click **Idle Maintenance** and select **Enable**.

- In the **Name** column, right-click **Regular Maintenance** and select **Enable**.



- From the **File** menu, select **Exit**.

Using the Contact Center Dashboard

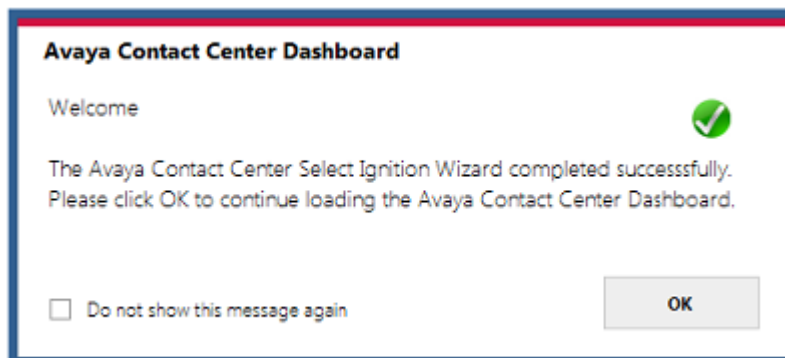
About this task

You can use the Contact Center Dashboard to access Contact Center system tools and diagnose system problems. The Contact Center Dashboard displays some Operating System and system details such as CPU type, network details, and Operating System activation status.

The Contact Center Dashboard launches automatically the first time the Contact Center server boots up.

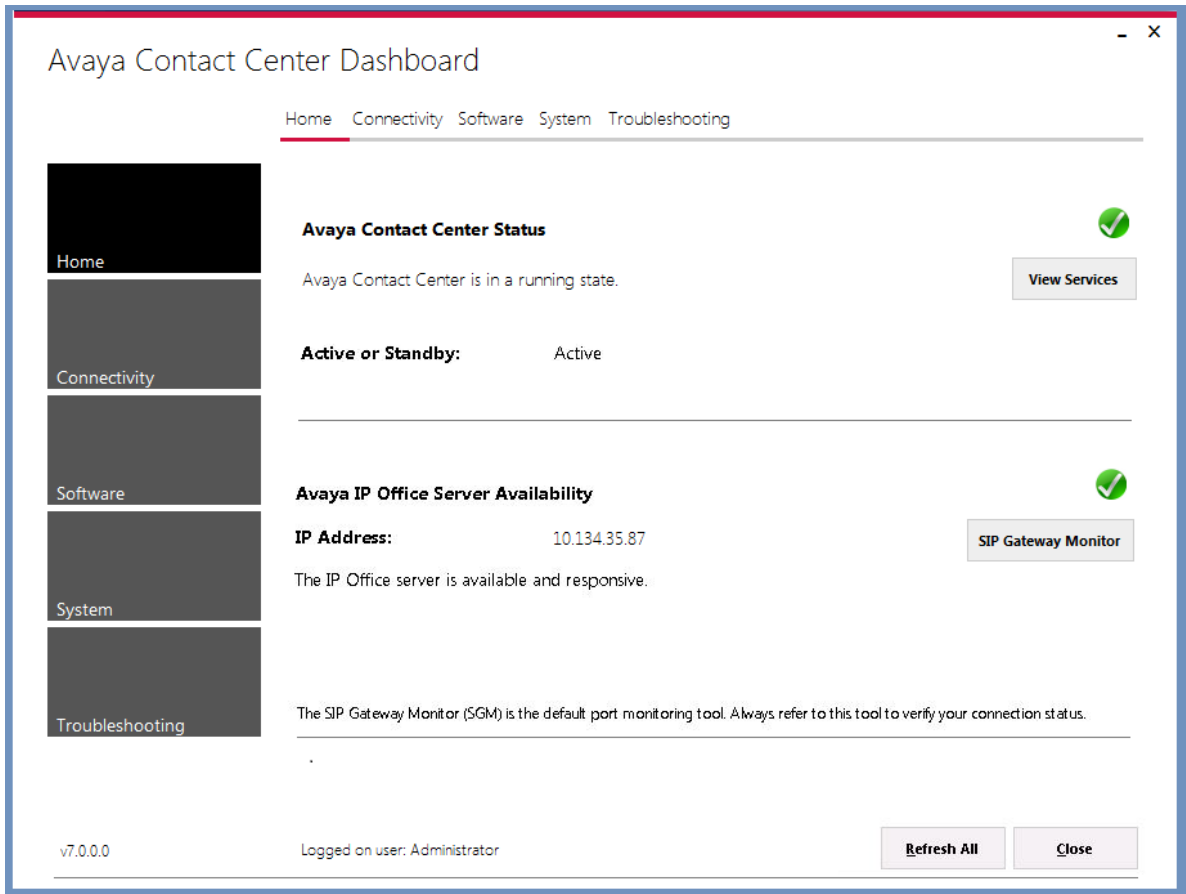
Procedure

- The Contact Center Dashboard Welcome message box automatically appears when the server starts up.



- Click **OK**.

3. On the Contact Center Dashboard, select the **Home** tab.



4. Click **Refresh All** to refresh the Contact Center Dashboard status reports.
5. In the **Avaya Contact Center Status** section, click **View Services** to monitor the state of the Contact Center Windows services.
6. In the **Avaya IP Office Server Availability** section, click **SIP Gateway Monitor** to determine if Contact Center is communicating with IP Office.

7. Select the **Connectivity** tab.

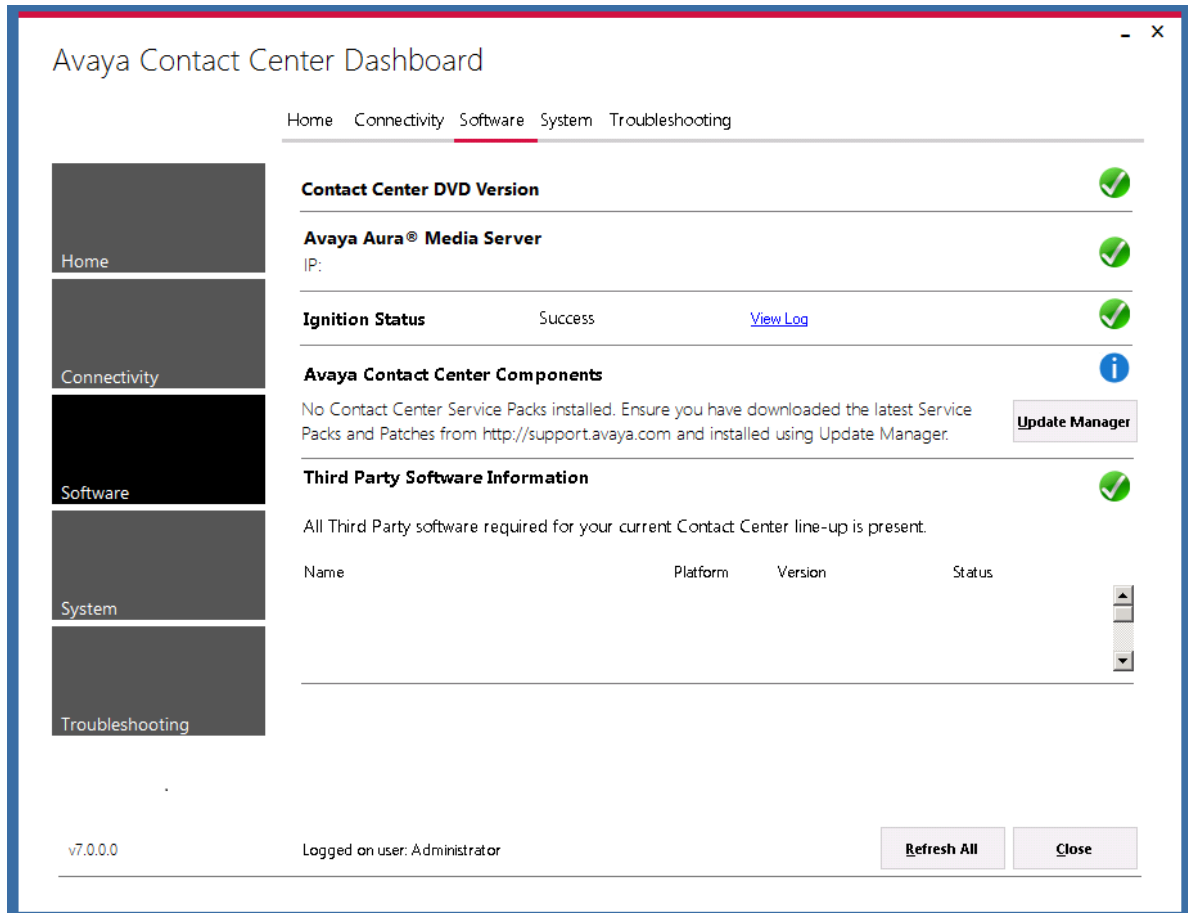
The screenshot shows the Avaya Contact Center Dashboard with the 'Connectivity' tab selected in the left-hand navigation menu. The main content area displays the following sections:

- SIP Gateway Monitor**: Monitor the status of the SIP connection to IP Office. **Launch** button (highlighted with a red box).
- Contact Center Multimedia Dashboard**: Monitor the multimedia mailbox status. **Launch** button.
- Contact Center Manager Administration**: Access Contact Center Manager Administration to configure and manage Contact Center resources. **Launch** button.
- System Control and Monitor Utility**: Monitor, stop, and start Contact Center services. **Launch** button.
- Contact Center License Manager**: Monitor license status and add additional licensed features. **Launch** button.
- Business Continuity Support**: Configure and control Business Continuity support feature for Contact Center. **Launch** button.

At the bottom of the dashboard, it shows 'v7.0.0.0' and 'Logged on user: Administrator'. There are 'Refresh All' and 'Close' buttons at the bottom right.

8. In the **SIP Gateway Monitor** section, click **Launch** to monitor the status of the SIP connection to IP Office.
9. In the **Contact Center Multimedia Dashboard** section, click **Launch** to monitor the multimedia mailbox status.
10. In the **Contact Center Manager Administration** section, click **Launch** to access Contact Center Manager Administration to configure and manage Contact Center resources.
11. In the **System Control and Monitoring Utility** section, click **Launch** to monitor, stop, and start Contact Center services.
12. In the **Contact Center License Manager** section, click **Launch** to monitor license status and add additional licensed features.
13. Select **Business Continuity Support** to configure the Business Continuity feature.

14. Select the **Software** tab.



15. **Contact Center Version** displays the version of the Contact Center software installed on the server.
16. **Avaya Aura® Media Server** displays the version of Avaya Aura® Media Server software installed on the server.
17. **Ignition Status** displays the Contact Center software installation status.
18. **Avaya Contact Center Components** displays the Contact Center software and patch line-up installed on the server.
19. **Third Party Software Information** displays the versions of the third-party software components used by Contact Center that are installed on the server.

20. Select the **System** tab.

The screenshot shows the Avaya Contact Center Dashboard with the 'System' tab selected. The dashboard includes a navigation menu on the left with options: Home, Connectivity, Software, System (selected), and Troubleshooting. The main content area displays the following system information:

- Machine Name:** ACCSONE
- Windows Domain:** aaccdomain.com
- Operating System:** Microsoft Windows Server 2012 R2 Standard
- Windows Activation Status:** Activated (with a green checkmark icon)
- RAM:** 17 % (16384 MB)
- CPU:** 1 % (2.926GHz 64bit Intel(R) Xeon(R) CPU X5647 @ 2.93GHz)
- Network:** (with a green checkmark icon)

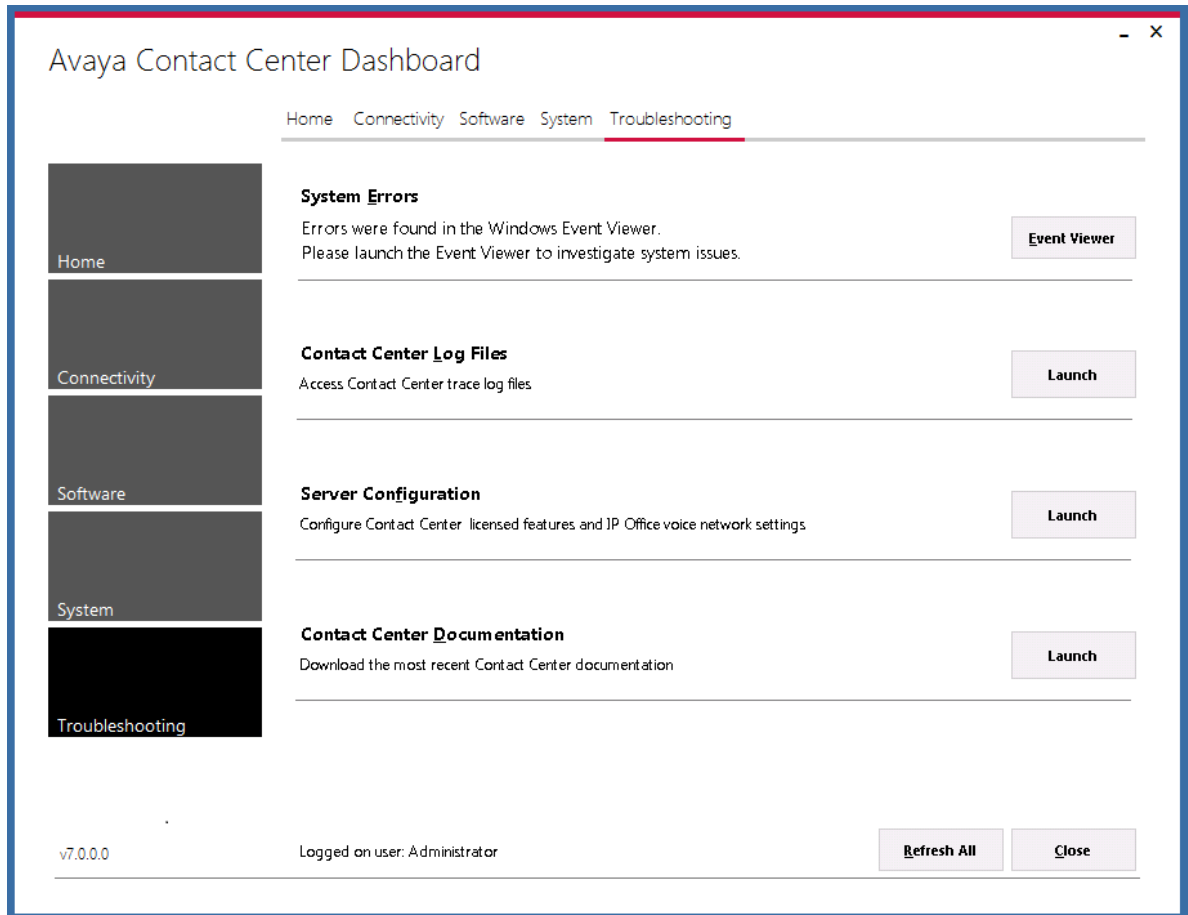
Name	IP Address	MAC Address
Local Area Connection	10.134.38.1	005056A067
- Hard Disks:** (with a green checkmark icon)

Name	Volume Name	Total Size GB	Free Space GB	Used
C:\				
D:\				
E:\				
G:\				

At the bottom of the dashboard, it shows 'v7.0.0.0' and 'Logged on user: Administrator'. There are 'Refresh All' and 'Close' buttons in the bottom right corner.

21. **Machine Name** displays the host name of the Contact Center server.
22. **Windows Domain** displays the name of the domain that the Contact Center server is in.
23. **Operating System** displays the Operating System version.
24. **Windows Activation Status** displays the Windows Operating System license and activation status.
25. **RAM** displays the amount of RAM memory in the server.
26. **CPU** displays the type of CPU in the server.
27. **Network** displays the networking details of the server: IP address and MAC address.
28. **Hard Disks** displays the number, size, and drive letter of the hard disk volumes in the server.

29. Select the **Troubleshooting** tab.



30. Select **System Errors** to access Contact Center events in the Microsoft Windows Event Viewer.
31. Select **Contact Center Log Files** to access Contact Center trace log files.
32. Select **Server Configuration** to configure Contact Center licensed features and IP Office voice network settings.
33. Select **Contact Center Documentation** to access and download the most recent Contact Center documentation from the Avaya support website.

Configuring IP Office for unsecured CTI connections

About this task

When you skip security configuration during Avaya Contact Center Select installation, by default Avaya Contact Center Select uses TCP for the CTI connection to IP Office. You cannot test a first call quickly until you configure IP Office to allow an unsecured CTI connection.

If Avaya Contact Center Select uses TLS to communicate with IP Office, you can skip this procedure.

Procedure

1. Using IP Office Manager, select **File > Advanced > Security Settings > System > Unsecured Interfaces**.
2. In the **Application Controls** section, select the **TAPI** check box.
3. Click **OK**.
4. Select **File > Save Security Settings**.

Next steps

Verify that the TCP connection between Avaya Contact Center Select and IP Office is connected. Open the **SIP Gateway Management Client** and verify that the **CTI Proxy** link **Transport** setting is **TCP** and that the link status is **CONNECTED**.

Configuring the Contact Center virtual machine

About this task

Configure the VMware resources for the Contact Center virtual machine. A virtual machine cannot have more vCPUs than the maximum number of physical CPUs on the host virtual server platform.

To adjust the virtual machine *Resource Allocations*, you must power off the virtual machine.

Before you begin

- Monitor the performance of the virtual machine.

Procedure

1. Using the vSphere client, select the **Inventory** view.
2. Locate the Contact Center virtual machine in the inventory navigation tree on the left. If not shown, select **View > Show VMs in Inventory**.
3. Click on the virtual machine.
4. Right-click on the virtual machine and select **Power > Shut Down Guest**.
Wait for the virtual machine to power off.
5. Right-click on the virtual machine and select **Edit Settings**.
6. Click the **Hardware** tab and select **CPUs**.
7. From the **Number of virtual sockets** list, select a value.
8. From the **Number of cores per sockets** list, select a value.
9. Click the **Hardware** tab and select **Memory**.

10. In the **Memory Size** box, increase the memory to at least 16 GB.
11. Click **OK**.
12. Right-click on the virtual machine and select **Edit Settings**.
13. Click the **Resources** tab and select **CPU**.
14. Select the **Reservation** slider and move it all the way to the right.
15. Click **OK**.
16. Click the **Resources** tab and select **Memory**.
17. Select the **Reservation** slider and then click on the orange triangle just below the slider.
18. Click **OK**.
19. Right-click on the virtual machine and select **Power** > **Power On**.
20. Continue to monitor the performance of the Contact Center virtual machine.

Configuring the virtual machine automatic startup settings

Before you begin

- Confirm that you have the proper level of VMware permissions to configure the automatic startup settings. If you do not have the proper level of VMware permissions, contact your system administrator.

About this task

When a vSphere ESXi host restarts or starts after a power failure, the virtual machines that are deployed on the host do not start automatically. All Contact Center virtual machines must be configured to start automatically when the vSphere ESXi host starts.

If the following virtual machines are deployed on the same ESXi host server, configure an automatic startup order for them:

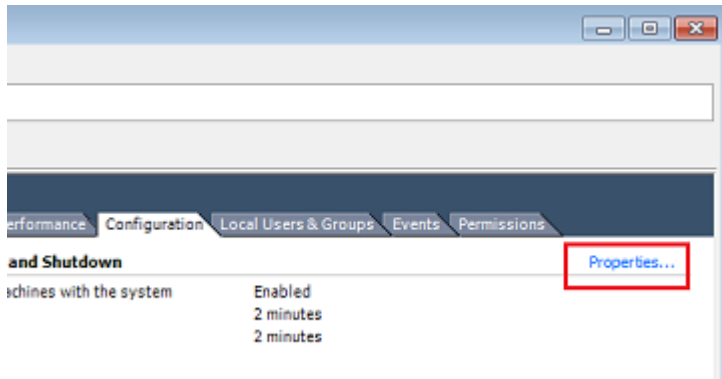
1. Avaya WebLM
2. Avaya Aura® Media Server
3. Contact Center

If these virtual machines are deployed on separate ESXi host servers, configure them to start up automatically and ensure they are high in the automatic restart order on their respective ESXi host servers.

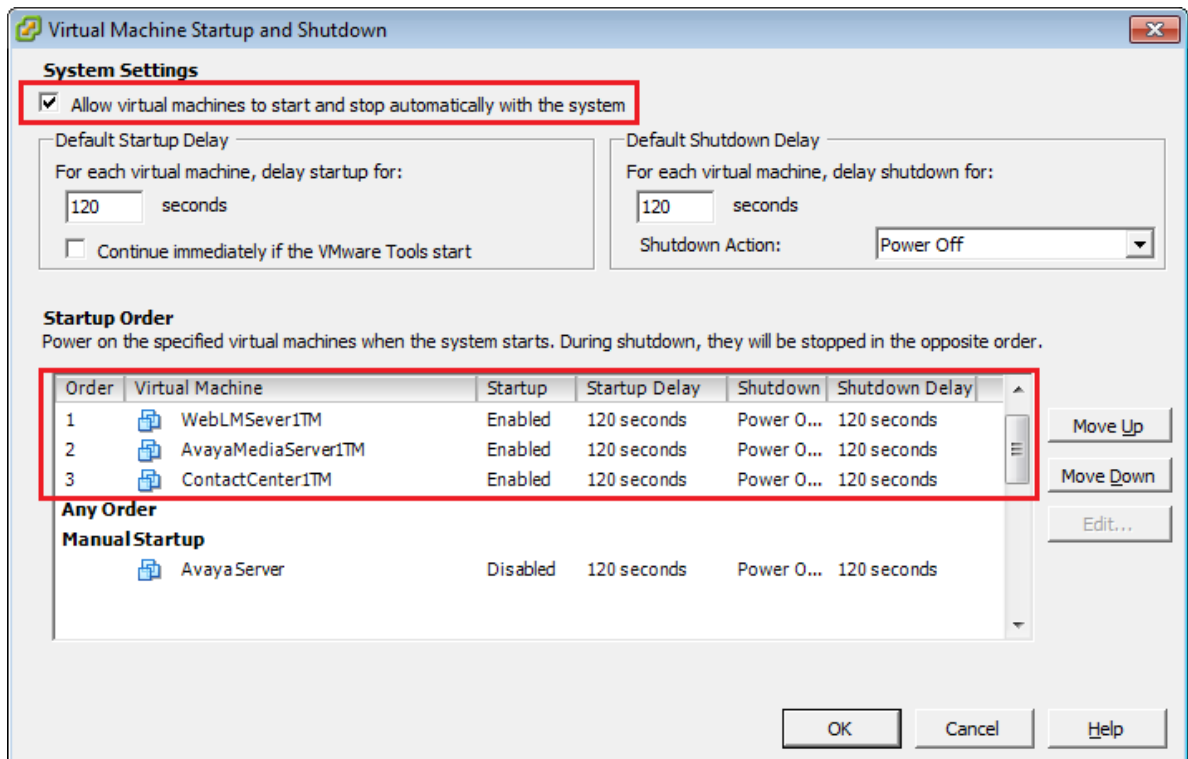
Procedure

1. In the vSphere Client inventory, select the host where the Contact Center virtual machines are located.
2. Click the **Configuration** tab.
3. In the **Software** section, click **Virtual Machine Startup/Shutdown**.

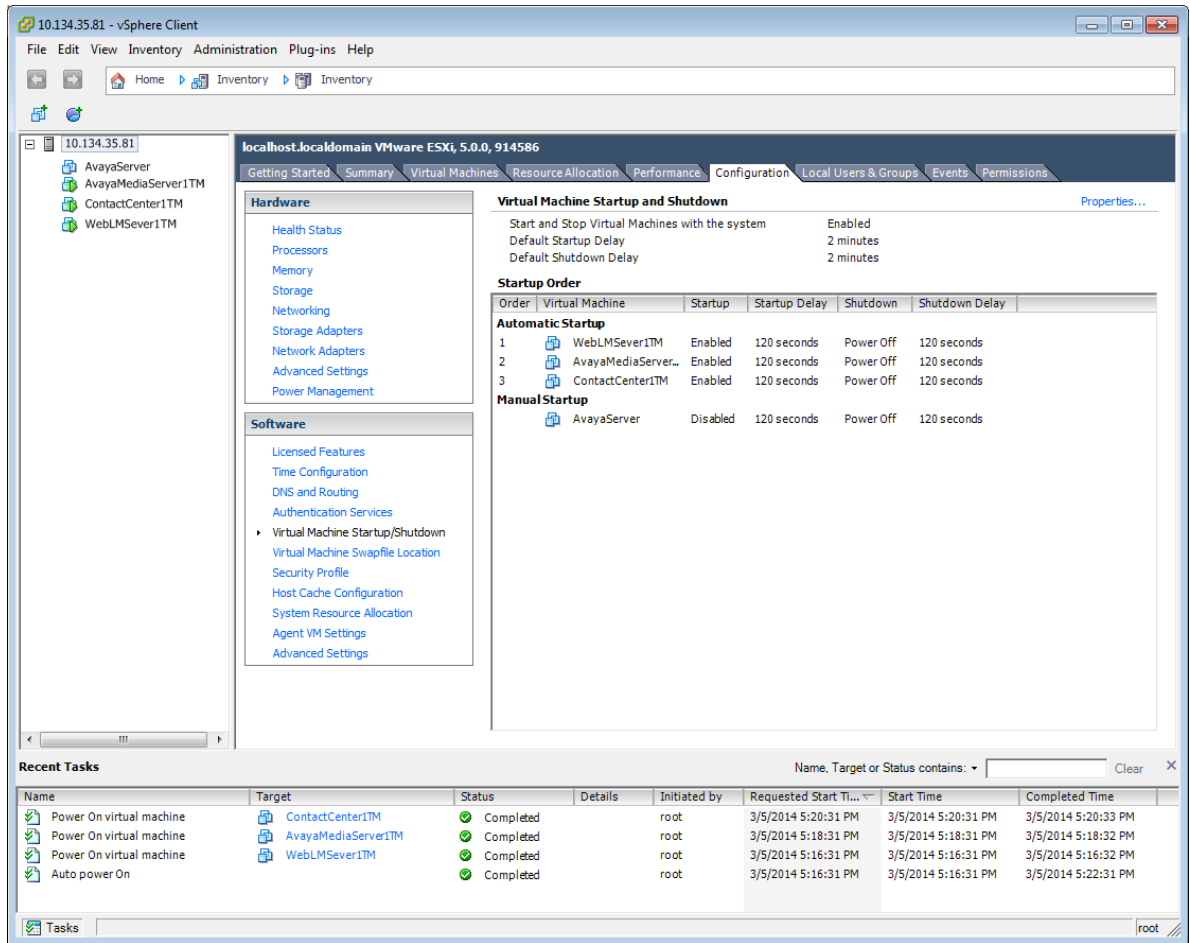
- Click **Properties** in the upper right corner of the screen.



- In the **System Settings** section, select **Allow virtual machines to start and stop automatically with the system**.
- In the **Manual Startup** section, select the WebLM virtual machine and using the **Move Up** button, move it to the top of the **Startup Order** list.
- In the **Manual Startup** section, select the Avaya Aura® Media Server virtual machine and using the **Move Up** button, move it to the second position on the **Startup Order** list.
- In the **Manual Startup** section, select the Contact Center virtual machine and using the **Move Up** button, move it to the third position on the **Startup Order** list.



9. Click **OK**.



Chapter 10: Deploying Avaya Workspaces on Avaya Contact Center Select Software Appliance

Avaya Workspaces is an optional browser-based application for agents. You can deploy and configure Avaya Workspaces as a part of the initial Avaya Contact Center Select installation or add Avaya Workspaces to your solution at a later stage.

For virtual installs, you must deploy a single-node Avaya Workspaces solution.

Important:

- The Avaya Workspaces cluster supports only 24-bit subnets (subnet mask 255.255.255.0). Ensure that all IP addresses of the Avaya Workspaces nodes belong to a 24-bit network.

You must use NTP servers to synchronize the time of the Avaya Workspaces cluster and the Contact Center environment. Set up the NTP servers before deploying or upgrading your Contact Center. You can use from one to three NTP servers, however, Avaya recommends that you use three NTP servers.

Virtual deployment during the initial installation

If you deploy Avaya Workspaces during the initial installation of Avaya Contact Center Select in a virtual environment, the installation sequence is the following:

1. Complete the Installation checklist details related to Avaya Workspaces and NTP servers. See [Avaya Workspaces installation checklist](#) on page 30.
2. Manually deploy one virtual machine using the Avaya Workspaces Open Virtual Appliance (OVA). See [Deploying the Avaya Workspaces OVA](#) on page 156.
3. When installing the Avaya Contact Center Select DVD software, select the Configure Workspaces check box. See [Installing Avaya Contact Center Select without Avaya Aura Media Server Release 7.1 DVD software](#) on page 129.
4. In the Ignition Wizard, configure the details for the Avaya Workspaces cluster and NTP servers. See [Configuring Avaya Workspaces during the initial installation](#) on page 158.

Virtual deployment at a later stage

You can add Avaya Workspaces to your solution at any stage using the Update Configurator. If you want to add Avaya Workspaces to an existing solution in a virtual environment, the installation sequence is the following:

1. Update your Contact Center to Release 7.1 Feature Pack 2 or later.

2. Complete the Installation checklist details related to Avaya Workspaces and NTP servers. In a single-node deployment, you need only one IP Address for the Avaya Workspaces node. See [Avaya Workspaces installation checklist](#) on page 30.
3. Manually deploy one virtual machine using the Avaya Workspaces Open Virtual Appliance (OVA). See [Deploying the Avaya Workspaces OVA](#) on page 156.
4. In the Update Configurator, configure the details for the Avaya Workspaces cluster and NTP servers. See [Adding Avaya Workspaces to an existing solution](#) on page 161.

Deploying the Avaya Workspaces OVA

Before you begin

Download the Avaya Workspaces OVA from the Avaya Support website at <https://support.avaya.com>.

Note:

If upgrading from a previously configured Avaya Workspaces installation, you must re-deploy the Avaya Workspaces cluster using the OVA, which is shipped with the latest release. Before you start deploying new virtual machines, shut down the virtual machines created from OVAs of the previous release.

About this task

Use this procedure to deploy optional Avaya Workspaces. Deploy the Avaya Workspaces OVA file onto a VMware ESXi host server using vCenter. This creates a virtual machine with the Avaya Workspaces software for use in the Contact Center solutions.

You must ensure that the Avaya Workspaces virtual machine meets or exceeds the following minimum specifications:

vCPU	Minimum CPU speed	Virtual memory reservation	Hard disk space	Number of NICs
8	2400 MHz	32 GB	500 GB	1 VMXNET3 Network Adapter

Important:

Use this procedure for virtual solutions only. If you deploy on a physical machine, ignore this procedure.

Procedure

1. In your vCenter client, select the host server on which to deploy the Avaya Workspaces OVA.
2. Select **File > Deploy OVF Template**.
3. On the **Source** window, click **Browse**.
4. On the **Open** message box, select the Avaya Workspaces OVA file.

5. Click **Open**.
6. On the **Source** window, click **Next**.
7. On the **OVF Template Details** window, verify the details of the Avaya Workspaces OVA template and click **Next**.
8. On the **End User License Agreement** window, read the license agreement, and if acceptable, click **Accept**.
9. Click **Next**.
10. On the **Name and Location** window, type the name of the new Avaya Workspaces virtual machine. This is not the server host name, this is the name of the VMware virtual machine as it appears in the VMware inventory.
11. Click **Next**.
12. On the **Host and Cluster** window, select the host server or cluster on which to deploy the Avaya Workspaces OVA. If you selected a cluster, select a **Specific Host** on that cluster.
13. Click **Next** to display the **Storage** window.
14. From the **Select a destination storage for the virtual machine files** list, select a location to store the Avaya Workspaces virtual machine image. Ensure that the storage location you select has sufficient available storage space to store a thick provisioned virtual machine image.
15. Click **Next**.
16. On the **Disk Format** window, select **Thin Provision**.
17. Click **Next**.
18. On the **Ready to Complete** window, verify the deployment settings. If you need to modify any of the settings, click **Back**.
19. Click **Power on after deployment**.
20. Log on to the Contact Center server using the default credentials.

The user name is `root` and the password is `root01`. You must not change the default credentials at this step. You can create a new password later when configuring Avaya Workspaces in the Ignition Wizard.
21. Enter the `# ifconfig` command to establish the name of your network adapter.
22. To open the network configuration script, enter the `# vi /etc/sysconfig/network-scripts/ifcfg-ens192` command. Ensure the network adapter name matches your environment.
23. Press the **Insert** key to enter the edit mode.
24. Modify the **IPADDR**, **GATEWAY**, **NETMASK** and **DNS** fields as required. Ensure the **BOOTPROTO** field is set to `none`.
25. To save the changes, press **Esc** and type `!wq!`. To exit without changes, press **Esc** and type `!q!`.

26. Enter the `# systemctl restart network` command to restart the network service and enable the changes.
27. In **VM Options**, under **VMWare tools** section, deselect the **Synchronize guest time with host** check box.

You must use NTP servers for time synchronization of Contact Center machines and Avaya Workspaces nodes. You can configure time synchronization settings while configuring Avaya Workspaces in the Ignition Wizard for fresh installs or in the Update Configurator for upgrades.

Configuring Avaya Workspaces during the initial installation

About this task

Use this procedure to configure Avaya Workspaces during the initial installation of Avaya Contact Center Select.

Procedure

1. On the Contact Center Ignition Wizard screen, select the **Workspaces** tab and configure the details.

The screenshot shows the 'Configuration Data' screen for Avaya Contact Center, specifically the 'Workspaces' tab. The screen is titled 'Avaya Contact Center' at the top. Below the title is the 'AVAYA' logo. The main heading is 'Configuration Data', followed by the instruction 'Enter the required configuration data.' There are several tabs: 'Core', 'Licensing', 'SIP', 'Multimedia', 'Workspaces' (selected), and 'Security Configuration'. The 'Workspaces' section contains a 'Cluster IP Address' field with an 'Add' button and a 'Remove' button. Below this is a 'Password' field and a 'Confirm Password' field. To the right, the 'LDAP Server' section has an 'IP Address' field, a 'Port' field, and a 'Protocol' dropdown menu. At the bottom, there is a 'Click Next to Continue' instruction and three buttons: '< Back', 'Next >', and 'Cancel'.

2. In the **Workspaces** section, click **Add** next to the IP Address box to add an IP address of the Avaya Workspaces node. Click **Remove** if you want to remove an IP address.

If you deploy Avaya Contact Center Select in a virtual environment, you must add one IP address.

3. In the **Workspaces** section, in the **Password** box, type the root password for the Avaya Workspaces nodes.

The password is checked against the server security policy for minimum password requirements. Avaya recommends that you enter a password that conforms to your corporate password policy.

*** Note:**

Do not use special symbols: @ # £ & ^.

4. In the **Confirm Password**, type the password again.
5. In the **LDAP Server** section, in the **IP Address** box, enter the IP address of the LDAP Server.

6. In the **Port** field, enter the port number of the LDAP protocol.
7. From the **Protocol** drop-down list, select a type of encryption you want to use:
 - TCP
 - TLS
8. Select the **Other settings** tab to configure NTP servers for time synchronization.

The screenshot shows the 'Configuration Data' window for Avaya Contact Center. The 'Other settings' tab is selected. The 'NTP Servers' section has an 'IP Addresses:' field with an 'Add' button and a 'Remove' button. The 'SSH session timeout:' field is set to '10 minutes'. The 'Cluster time zone' section shows the 'Windows time zone' as '(UTC+00:00) Dublin, Edinburgh, Lisbon, London' and a drop-down menu for the 'Linux cluster time zone'.

9. In the **NTP Servers** section, click **Add** to add an IP address of an NTP server.

You can add up to three IP addresses. To remove the IP address, select the required IP address and click **Remove**.
10. In the **SSH session timeout** box, type the timeout value in minutes.

The default value is 10 minutes. You can enter the value from 5 to 60 minutes.
11. In the **Cluster time zone** section, from the drop-down list, select the time zone of the Linux cluster.

Avaya recommends that you use the appropriate time zone of the Windows system. You can view the current Windows time zone on the same screen.
12. Click **Next**.

Adding Avaya Workspaces to an existing solution

About this task

You can add Avaya Workspaces to your current solution at any stage using the Contact Center Update Configurator.

Before you begin

- Ensure that your Contact Center is licensed for Avaya Workspaces.
- Update your Contact Center to Release 7.1 Feature Pack 2 or later.
- Complete the Installation checklist details related to Avaya Workspaces and NTP servers. See [Avaya Workspaces installation checklist](#) on page 30.
- Manually deploy one virtual machine using the Avaya Workspaces Open Virtual Appliance (OVA). See [Deploying the Avaya Workspaces OVA](#) on page 156.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Update Configurator**.
The Contact Center Update Configurator opens.
3. On the **Configure Workspaces** tab, next to the **IP Address** box, click **Add**.
For Avaya Contact Center Select Software Appliance, you must add one IP address.
To remove an IP address, select an address and click **Remove**.
4. In the **Cluster IP** field, enter the IP address of the Avaya Workspaces cluster.
5. In the **Password** box, type the root password for the Avaya Workspaces cluster.
The password is checked against the server security policy for minimum password requirements. Avaya recommends that you enter a password that conforms to your corporate password policy.

 **Note:**

Do not use special symbols: @ # £ & ^.

6. In the **Confirm Password** box, retype the password.
7. **(Optional)** To ensure that passwords match, select the **Show password** check box.
8. In the **LDAP IP Address** box, type the IP address of the LDAP server.
9. In the **Port** field, enter the port number of the LDAP protocol.
10. From the **Protocol** list, select one of the following encryption types:
 - TCP
 - TLS
11. To configure NTP servers for time synchronization, select the **Other settings** tab.

12. To add an IP address of an NTP server, next to the **IP Address** box, click **Add**.
You can add up to three IP addresses.
To remove an IP address, select an address and click **Remove**.
13. In the **SSH session timeout** box, type the timeout value in minutes.
The default value is 10 minutes. You can enter the value from 5 to 60 minutes.
14. From the **Linux cluster time zone** list, select the time zone of the Linux cluster.
Avaya recommends that you use the appropriate time zone of the Windows system. You can view the current Windows time zone on the same screen.
15. Click **Configure**.
16. When the Contact Center Update Configurator completes the configuration process, click **Yes** to restart the server.

Part 3: User Contact Recording configuration

Chapter 11: User Contact Recording Pause and Resume configuration

Avaya Contact Center Select supports IP Office Call Recording. IP Office Call Recording provides regulatory type recording, including the option to pause automatic recording for Payment Card Industry (PCI) security compliance. Avaya Contact Center Select supports the Call Recording pause and resume feature when it is initiated from a physical phone set. The Agent Desktop user interface does not have a pause button. Agents and agent supervisors must use their physical phone to pause and resume voice contact recording.

If your Avaya Contact Center Select agents and agent supervisors must be able to pause contact recording, add a Pause Recording button to each of their associated IP Office users.

Using IP Office Manager

Before you begin

- Install the IP Office Manager software on a client computer.
- Ensure the client computer can communicate with the IP Office server.

About this task

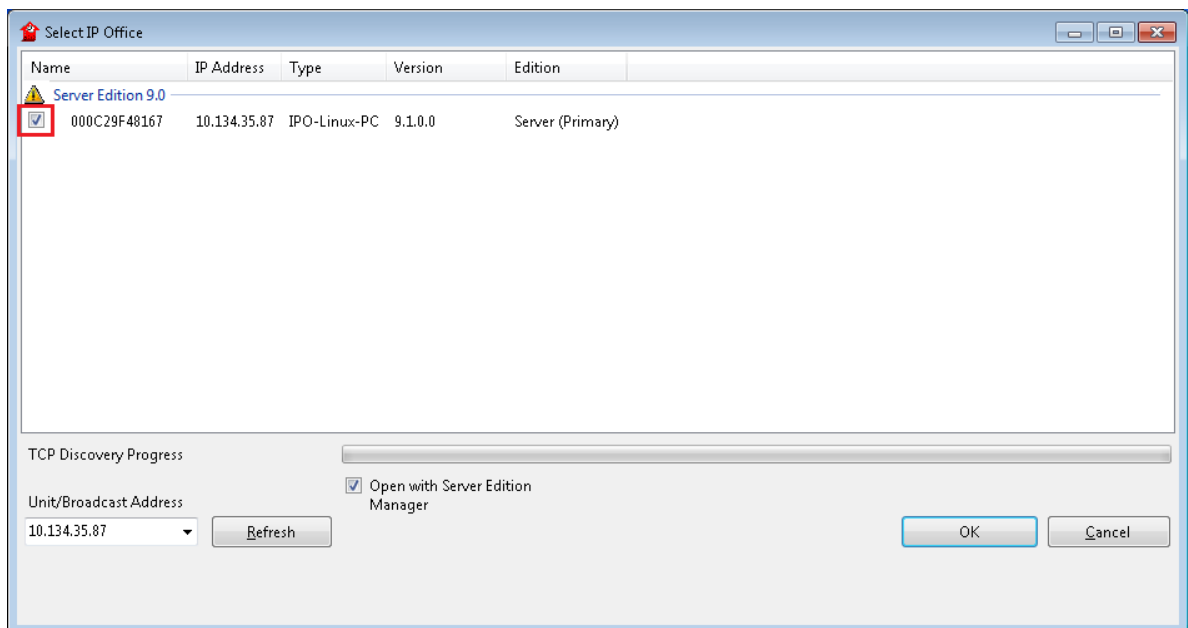
IP Office Manager is a component of the IP Office administration suite of applications. You use IP Office Manager to configure IP Office. IP Office Manager runs on a Windows computer and connects to the IP Office system using an Ethernet LAN connection.

IP Office Manager is an off-line editor. Use IP Office Manager to connect to your IP Office server and retrieve a local copy of the IP Office current configuration settings. You can then edit the local copy of the IP Office configuration and when you are ready, save your updated configuration data back to the IP Office server.

Procedure

1. On the client computer, select **Start > All Programs > IP Office > Manager**.
2. On the **Configuration Service User Login** message box, in the **Service User Name** box, type the user name. The default name is Administrator.
3. In the **Service User Password** box, type the user password. The default password is Administrator.

4. From the menu, select **File > Close Configuration**. This closes any open and potentially out-of-date configurations.
5. To retrieve the current (most recent) IP Office configuration settings, from the menu, select **File > Open Configuration**.
6. In the **Select IP Office** window:
 - If the required IP Office server is listed, use the check box to select your IP Office server from the list of available servers.
 - If the required IP Office server is not listed, in the **Unit/Broadcast Address** box type the IP address for your IP Office server. Click **Refresh** to perform a new search. The IP Office server then appears in the list of available servers. Use the check box to select your IP Office server from the list of available servers.



7. Click **OK**.
8. On the **Configuration Service User Login** message box, in the **Service User Name** box, type the user name. The default name is Administrator.
9. In the **Service User Password** box, type the user password. The default password is Administrator.
10. IP Office Manager opens and displays the current configuration data for your IP Office server.

Configuring a Pause Recording button for users

Before you begin

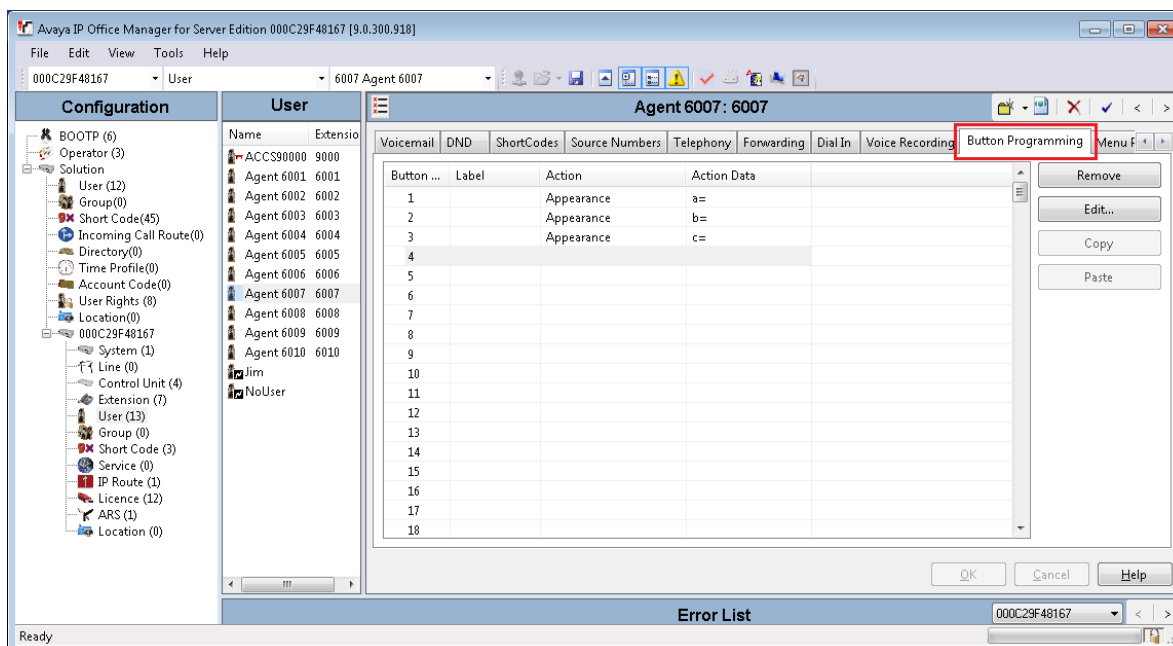
- Ensure the Contact Recorder application is installed, configured, and working on your IP Office. For more information about Contact Recorder, see *Installing Contact Recorder for IP Office* on the Avaya Support website at <http://support.avaya.com>.

About this task

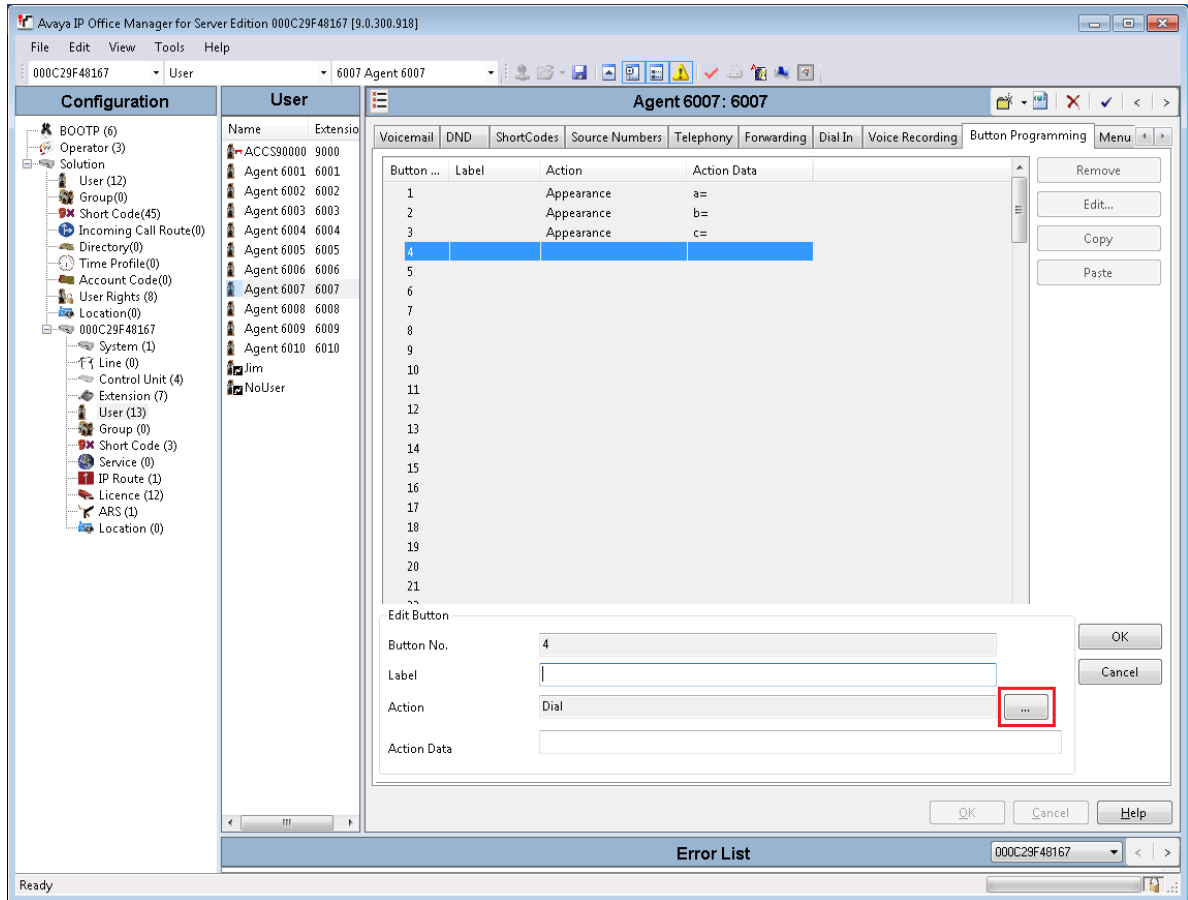
Configure a Pause Recording button for each Avaya Contact Center Select (agent and agent supervisor) user. The button status indicates when call recording is paused. Pressing the button again restarts call recording. The IP Office system can also automatically restart recording after a set delay.

Procedure

1. Using IP Office Manager, select the IP Office server in the **Configuration** pane.
2. In the **Configuration** pane, select your IP Office server.
3. In the left pane, select **User** and select the individual user.
4. In the right pane, select the **Button Programming** tab.

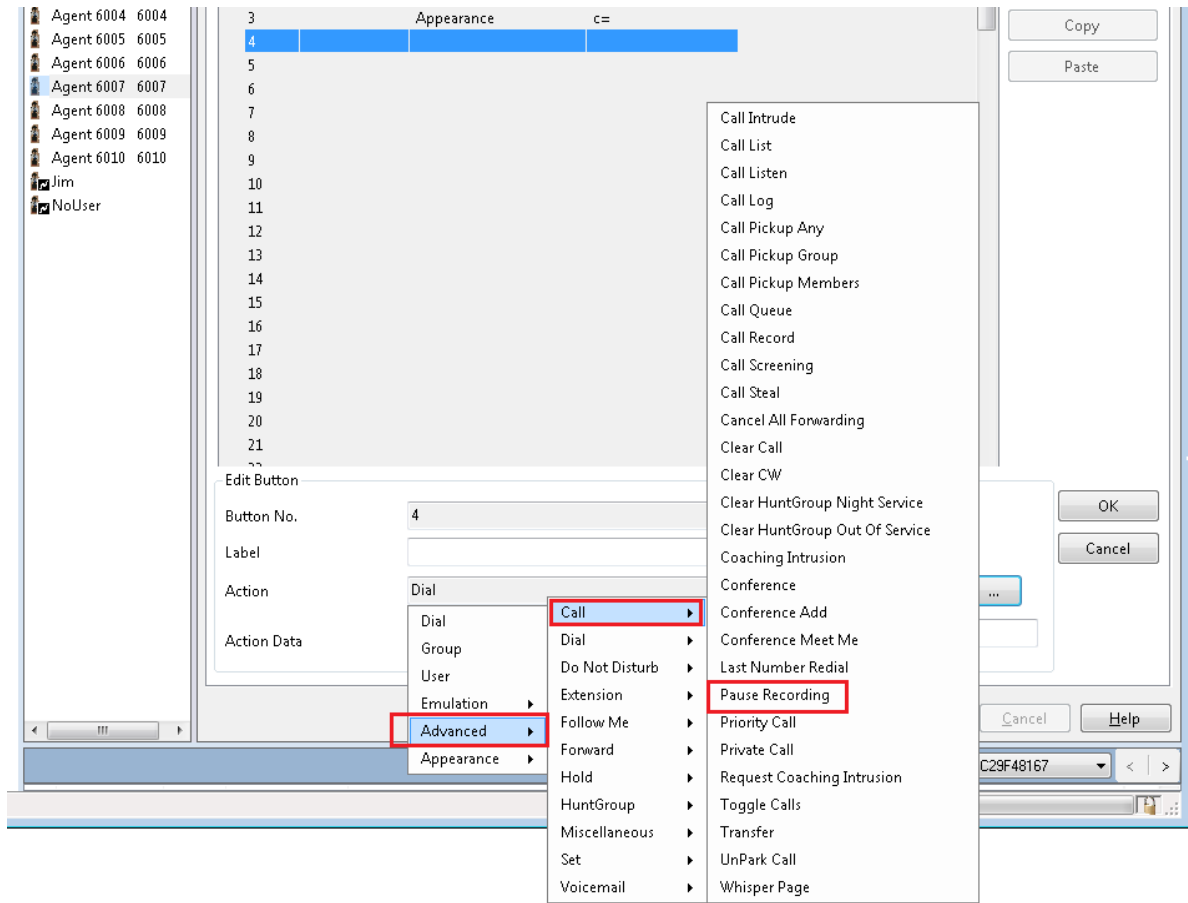


- From the user **Button** list, select the number of the button on which you want to program Pause Recording and click **Edit**.

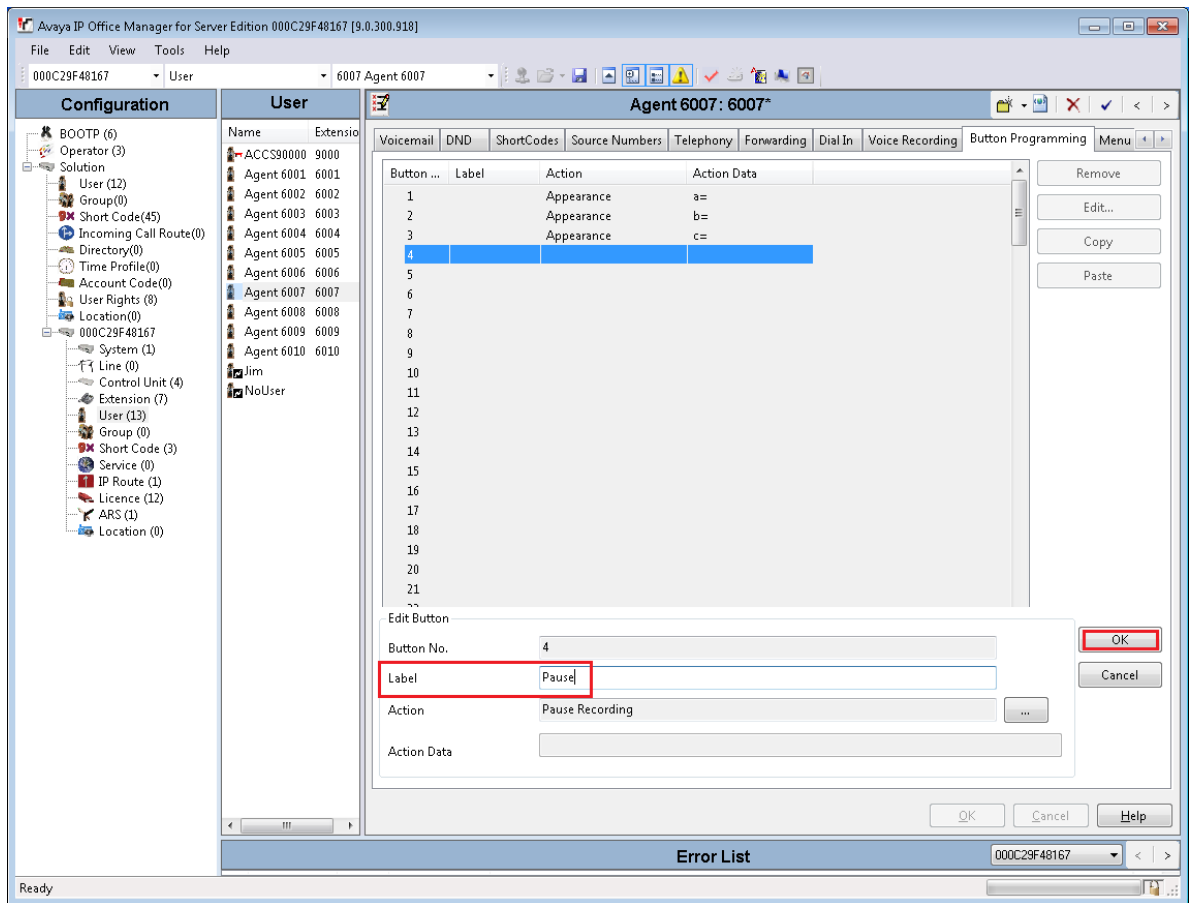


- In the **Edit Button** section, click the **Action** browse “...” button.

7. Select **Advanced > Call > Pause Recording**.

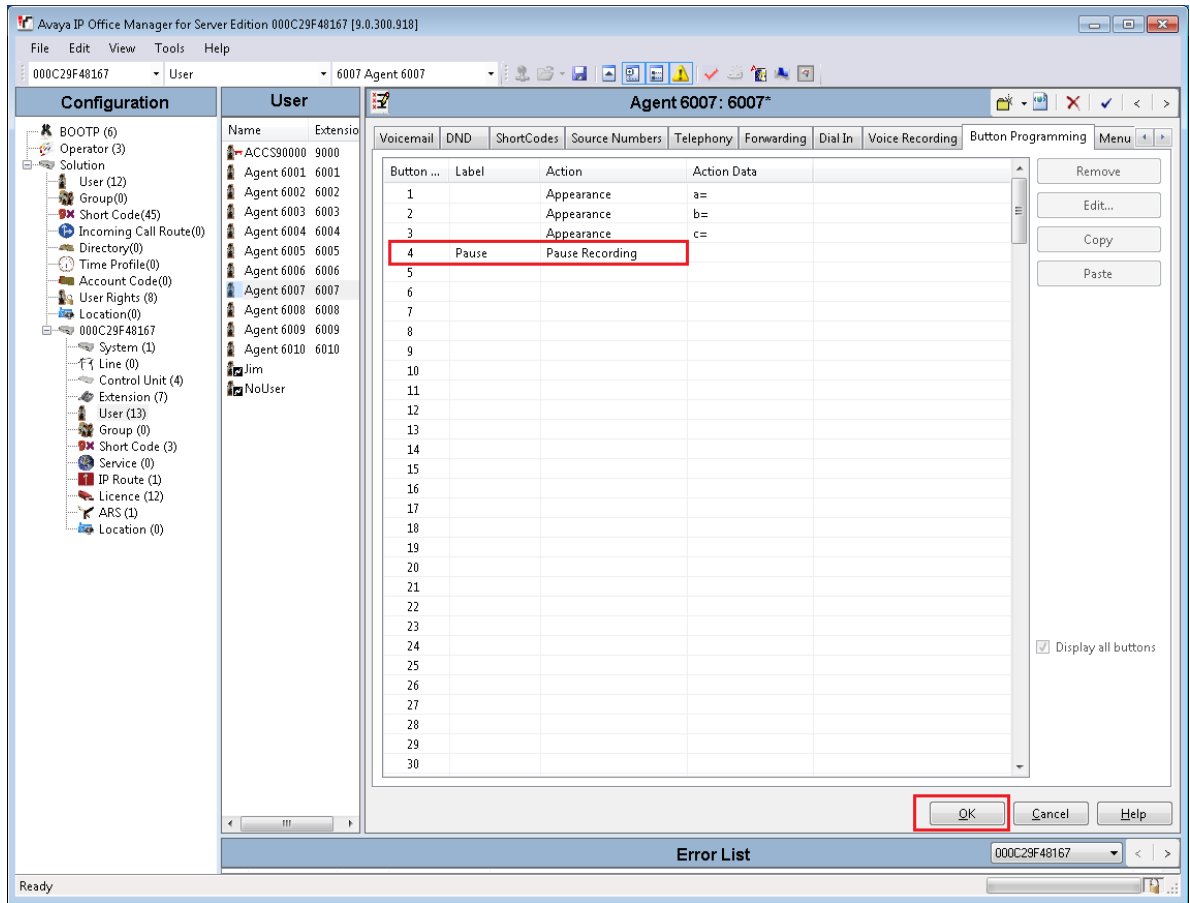


8. In the **Label** box, type a description to appear on the telephone display.



9. Click **OK**.

10. On the **Button Programming** tab, click **OK**.



11. Repeat this procedure for each IP Office user that represents an Avaya Contact Center Select agent or agent supervisor. Avaya recommends that you configure Pause Recording on the same button number for all users. Avaya recommends that you label each Pause Recording button with the same description.
12. Continue to add a Pause Recording button to each new IP Office user that represents a new Avaya Contact Center Select agent or agent supervisor.

Configuring the Contact Recording Auto Restart Delay

Before you begin

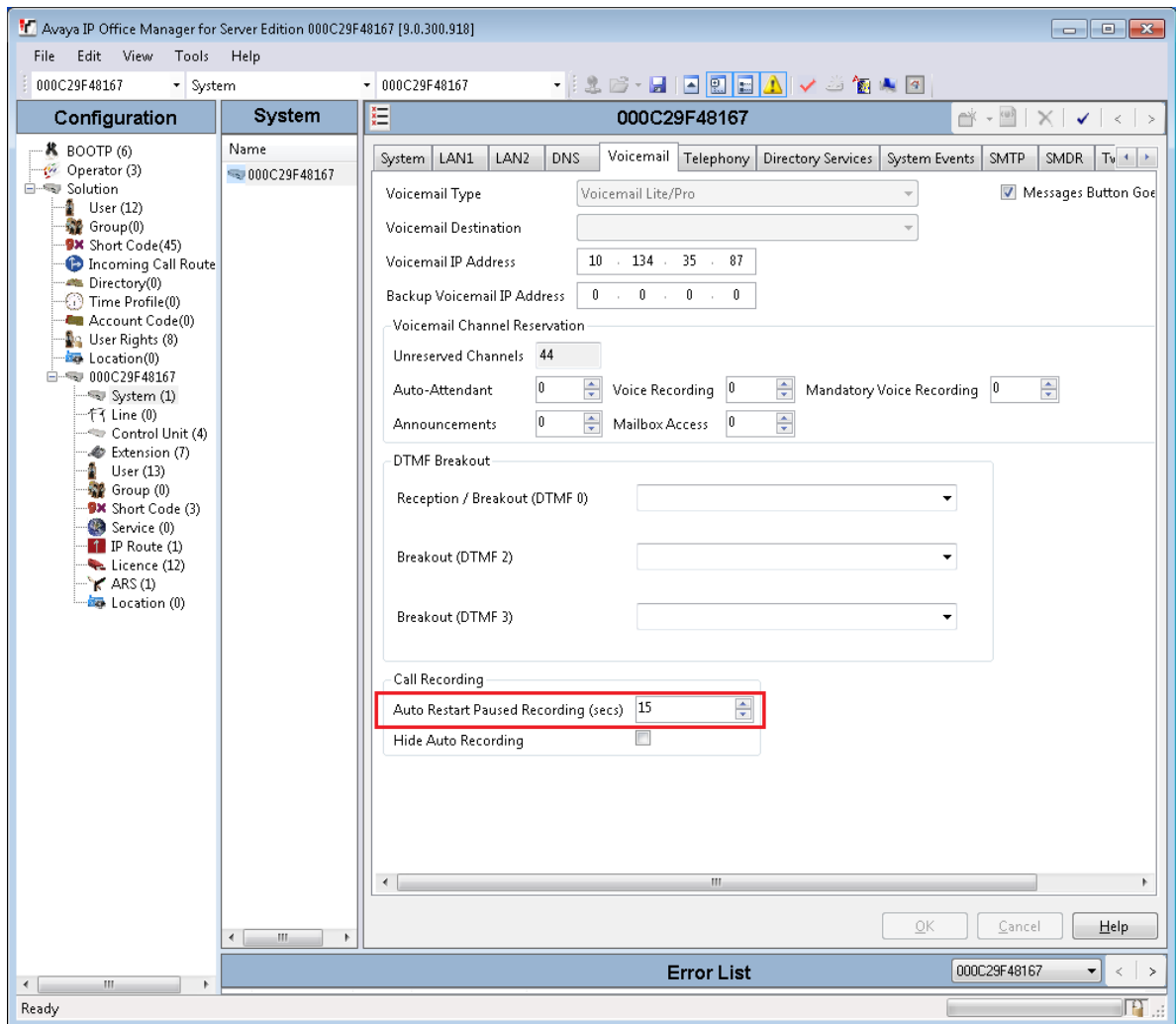
- Ensure the Contact Recorder application is installed, configured, and working on your IP Office. For more information about Contact Recorder, see *Installing Contact Recorder for IP Office* on the Avaya Support website at <http://support.avaya.com>.

About this task

By default, Contact Recording automatically restarts a paused recording after 15 seconds. Configure the Auto Restart Paused Recording setting for your solution.

Procedure

1. Using IP Office Manager, select the IP Office server in the **Configuration** pane.
2. In the **Configuration** pane, select your IP Office server.
3. In the left pane, click **System**.
4. Click the **Voicemail** tab.
5. Set **Auto Restart Paused Recording** to the required time in seconds.



6. Click **OK**.

Saving the IP Office configuration data

Before you begin

- Install the IP Office Manager software on a client computer that can communicate with the IP Office server.

About this task

Use IP Office Manager to save your configuration changes to the IP Office server.

Procedure

1. In IP Office Manager, in the **Configuration** pane, select your IP Office server.
2. From the main IP Office Manager menu, select **File > Save Configuration**.
3. On the **Send Multiple Configurations** window, use the check box to select your IP Office server from the list.
4. Click **OK**.

IP Office Manager saves the offline configuration file to your IP Office server.

Part 4: Reverse proxy for Avaya Workspaces

Chapter 12: Solution overview

You can configure the reverse proxy functionality for Avaya Workspaces. With this functionality, remote agents and supervisors located outside the contact center infrastructure can access Avaya Workspaces and perform their tasks without VPN connection.

Important:

Avaya Workspaces for Avaya Contact Center Select does not support WebRTC-enabled agents. To handle voice calls, Avaya Workspaces remote agents must use Avaya softphones or hardphones being logged in as remote workers.

This chapter describes how to configure the remote access to Avaya Workspaces using the Avaya Session Border Controller for Enterprise reverse proxy feature.

A reverse proxy is a web server that terminates connections with clients and makes new connections to back-end servers on their behalf. When you enable the reverse proxy for Avaya Workspaces using Avaya Session Border Controller for Enterprise, remote agents and supervisors can access Avaya Workspaces without VPN connection.

This part does not include information about deployment and configuration of the following products:

- Avaya Contact Center Select with Avaya Workspaces
- Avaya Aura[®] Media Server
- Avaya Session Border Controller for Enterprise
- Softphones or hardphones for remote workers

For more information about deployment and configuration of the above-mentioned products, see the corresponding product documentation at <https://support.avaya.com>.

Supported contact types

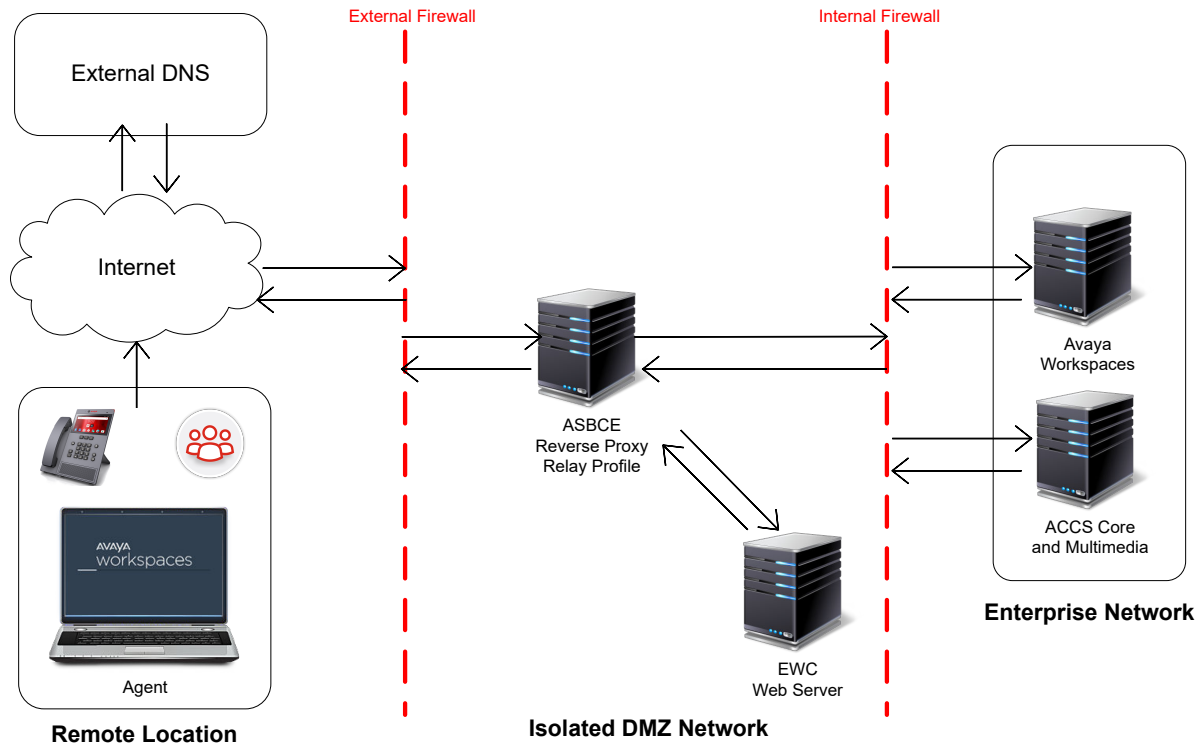
Avaya Workspaces supports the remote worker functionality for the following contact types:

- Web Chat
- Email
- Voice (using remote worker hard- or softphone)
- Outbound
- Generic Channel (contacts created inside the enterprise network)

Architecture overview

You can configure reverse proxy on Avaya Session Border Controller for Enterprise to allow external agents to access Avaya Workspaces from a remote location.

The following diagram shows an example of the remote agent solution architecture:



The following are the considerations for the reverse proxy for Avaya Workspaces:

- The implementation requires a split-horizon DNS where both external and internal agents use the same FQDNs to access Avaya Workspaces. The FQDNs resolve to different IPs depending on whether the agent is remote or on-premise.
- Only one external (internet-facing) IP address is required. Externally, all required FQDNs resolve to the single IP and are routed internally to the correct Avaya Workspaces server/cluster based on an URL.
- Configure an external firewall with the following items:
 - One external IP address on the external (WAN) side.
 - One internal IP address on the internal (LAN) side.
- Avaya Session Border Controller for Enterprise requires the following available items:
 - One IP on the external (B1) side.
 - One IP on the internal (A1) side.

- Configure an internal firewall with the following items:
 - One externally facing IP address on the external (WAN) side.
 - One internally facing IP address on the internal (LAN) side.

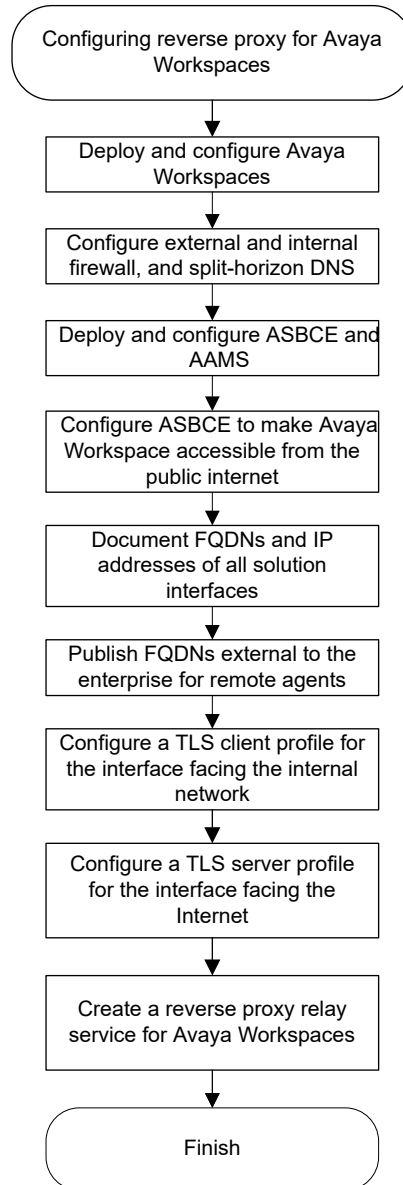
Prerequisites

Before you configure the remote access through reverse proxy, do the following:

- Deploy and configure Avaya Workspaces for all required channels.
- Ensure that internal agents can log in to Avaya Workspaces and process contacts.
- Deploy the following applications:
 - Avaya Aura® Media Server
 - Avaya Session Border Controller for Enterprise
- Configure split-horizon DNS for your solution so that both internal and remote agents can use the same FQDNs to access Avaya Workspaces. However, the FQDNs resolve to different IP addresses depending on whether the agent is remote or on-premise.
- Configure the external firewall to NAT requests on all required ports through to the Avaya Session Border Controller for Enterprise.
- Configure the internal firewall to route requests through to Avaya Workspaces using the NAT functionality.

Reverse proxy configuration process flow

The following workflow shows the sequence of tasks that you must perform to deploy the reverse proxy for remote access to Avaya Workspaces:



Configuration and deployment details

To enable remote access to Avaya Workspaces for agents outside your enterprise network, you must gather all configuration and deployment details.

Documentation of FQDNs and IP addresses of solution interfaces

To configure remote access to Avaya Workspaces, you must document FQDNs and IP addresses of Avaya Workspaces interfaces that remote agents access during normal operation.

Publishing of FQDNs external to the enterprise for remote agents

Avaya Workspaces users use FQDNs to access the functionality in the solution. In the enterprise network, FQDNs are resolved to the IP addresses through the internal Domain Name Server (DNS). For example, Avaya Workspaces users access Avaya Workspaces cluster FQDN to log in and receive basic user functionality depending on the agent footprint size.

Similar to on-premise workers, remote agents must also be able to utilize the same URLs and client requests, even though they are outside of the enterprise. To allow external users to access Avaya Workspaces, the Avaya Workspaces FQDN must resolve to the Listen IP on the external firewall. Therefore, on the external-facing DNS server, a customer must publish an entry for each required Avaya Workspaces FQDN that remote agents use. The number of FQDNs for publishing depends on customer configuration.

When a remote agent accesses or requests a URL containing the Avaya Workspaces FQDNs, the FQDNs are resolved to a single IP, which is the external firewall Listen IP address.

Function and role of the external firewall for remote agents

All remote agent requests terminate on a single IP address on the external firewall. With the configuration rule on the firewall, the requests are translated into internal addresses and ports by using Network Address Translation (NAT). Customers must configure their external firewall to translate requests coming in on different ports towards the next application in the chain, which is the reverse proxy. The external firewall allows the requests to go to the reverse proxy.

The reverse proxy forwards the requests to the unique IP address and port to the internal firewall based on the path in the request URL.

Configure the external firewall to NAT requests on all required ports through to the Avaya Session Border Controller for Enterprise.

Instead of port 443, Avaya Workspaces uses non-standard ports, so the external firewall must use either HTTP or HTTPS depending on the Avaya Workspaces configuration:

- port 31390 and HTTPS if Avaya Workspaces security is enabled
- port 31380 and HTTP if Avaya Workspaces security is disabled

Function and role the reverse proxy for remote agents

The reverse proxy determines which URL requests must be allowed and how the requests must flow into the enterprise applications. It also relays the reverse communications to remote agents.

The reverse proxy is configured with a set of rules that analyze the request URLs and allow the requests to go to the backend servers.

Reverse proxy policies, TLS profiles, and relay services

Avaya Session Border Controller for Enterprise and reverse proxy perform many essential functions that must be appropriately configured on each deployment:

- Many whitelist relays require a WebSocket connection. Therefore, on Avaya Session Border Controller for Enterprise, you must create a reverse proxy policy with WebSockets enabled.
- Session Border Controller reverse proxy relay requires the following:
 - A TLS client profile for the interface facing the internal Intranet Avaya Workspaces servers/clusters
 - A TLS server profile for the interface facing the Internet
- For each server/cluster:port combination, you must configure a reverse proxy relay service. For multiple servers using the same port, such as 443, Avaya Session Border Controller for Enterprise directs the requests to the appropriate back-end server/cluster based on the URL in the request.

Instead of port 443, Avaya Workspaces uses non-standard ports, so the server profile must use either HTTP or HTTPS depending on the Avaya Workspaces configuration:

- port 31390 and HTTPS if Avaya Workspaces security is enabled
- port 31380 and HTTP if Avaya Workspaces security is disabled

Function and role of the internal firewall

An internal firewall is the final application before the enterprise applications. On its external (WAN) side, the internal firewall communicates with various IP addresses and ports allocated to Avaya Workspaces servers/clusters. Using the NAT functionality and preconfigured rules, it routes all allowed requests through to the servers on the internal network.

Configure your internal firewall to route requests through to Avaya Workspaces using the NAT functionality.

Connectivity details of remote agents

Remote agents connect to Avaya Workspaces similar to how they connect within the enterprise.

Remote agents do not need to log in to an Enterprise VPN to access the Avaya Workspaces application.

Similar to on-site agents, remote agents must use Avaya softphones or hardphones to handle voice and video contacts.

Example of remote agents accessing Avaya Workspaces

A remote agent opens a supported browser and accesses the URL for Avaya Workspaces.

For example, `https://<Avaya Workspaces Cluster FQDN>/services/UnifiedAgentController/workspaces/`.

Based on the externally published FQDNs, the FQDN is resolved to the external firewall IP address and the request is directed to the external firewall. Functions of the external firewall are:

- External firewall allows the requests from remote agents through to the reverse proxy.
- Reverse proxy already has the configuration information set up to allow the requests to be processed securely. After checking the validity of the requests, the requests are forwarded to an internal IP address and port destination on the internal firewall.

Remote worker phone set configuration

Remote Avaya Workspaces agents can handle voice calls using Avaya softphones or hardphones and being logged in as remote workers.

To configure remote worker softphones or hardphones for your Avaya Workspaces agents, follow the instructions in the latest release of *Administering Avaya Session Border Controller for Enterprise* at <https://support.avaya.com>.

Chapter 13: Avaya Session Border Controller for Enterprise configuration

To enable reverse proxy for Avaya Workspaces, you must first configure Avaya Session Border Controller for Enterprise (Avaya SBCE) to enable calls from the public internet. Therefore, you must install Avaya SBCE as part of your solution. For information about how to install Avaya SBCE, see the Avaya SBCE deployment guide applicable for your solution at <https://support.avaya.com/>.

For information about how to configure Avaya SBCE to enable calls from the public internet, complete the tasks described in this section.

Configuring Avaya SBCE networks

About this task

Use this procedure to configure Avaya SBCE networks settings.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Networks & Flows > Network Management > Interfaces**.
3. On the Interfaces page, enable the following interfaces:
 - A1 internal interface
 - B1 external interface
4. On the Networks tab, configure the following networks:
 - A1 internal network
 - B1 external network

Creating a reverse proxy policy

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Configuration Profiles > Reverse Proxy Policy**.
3. Click **Add**.
4. In the **Rule Name** field, type the name of the reverse proxy policy and click **Next**.
5. In the General area, select the **Allow Web Socket** check box.
6. Keep the default values in the other fields.
7. Click **Finish**.

Deploying Identity Certificate on Avaya SBCE

Creating the common client certificate

About this task

Use this procedure to create the common client certificate that you require while creating a client profile for Avaya Workspaces.

Procedure

1. Create an end entity by performing the following steps:
 - a. On the System Manager web console, click **Services > Security > Certificates > Authority**.
 - b. In the navigation pane, in the RA Functions section, click **Add End Entity**.
 - c. In the **End Entity Profile** field, select `INBOUND_OUTBOUND_TLS`.
 - d. In the **Username** field, enter a user name.
For example, SBCINT.
 - e. In the **Password (or Enrollment Code)** field, enter a password.
Ensure that you make a note of the user name and password. The user name and password are required when creating a certificate for this server.
 - f. In the **Confirm Password** field, re-enter the password.
 - g. In the **CN, Common name** field, enter the FQDN of Session Border Controller.
For example, Subject: CN=workspaces.acc.avaya.com, OU=SDP, O=AVAYA, C=US

- h. In the **IP Address** field, enter the IP address of the Session Border Controller internal interface.
 - i. In the **Token** field, select `P12` file.
 - j. Click **Add**.
2. Create a keystore by performing the following steps:
- a. On the System Manager web console, click **Services > Security > Certificates > Authority**.
 - b. In the navigation pane, click **Public Web**.
 - c. On the EJBCA welcome page, in the navigation pane, click **Create Keystore**.
 - d. On the Keystore Enrollment page, enter the user name and password that you specified while creating the end entity.
 - e. Click **OK**.
 - f. Select the **Key Length** as 2048 bits.
 - g. Click **Enroll**.
 - h. Save the certificate file.

Creating the common server certificate

About this task

Typically, a public Certificate Authority is used to generate a common server certificate. However, if you cannot use a public CA, you can use System Manager to create a certificate. When using a common server certificate created in System Manager, ensure that you add System Manager as a trusted certificate authority on every agent's PC.

Use this procedure to create the common server certificate that you require while creating a server profile for Avaya SBCE.

Procedure

1. Create an end entity by performing the following steps:
 - a. On the System Manager web console, click **Services > Security > Certificates > Authority**.
 - b. In the navigation pane, in the RA Functions section, click **Add End Entity**.
 - c. In the **End Entity Profile** field, select `INBOUND_OUTBOUND_TLS`.
 - d. In the **Username** field, enter a user name.
For example, SBCEXT.
 - e. In the **Password (or Enrollment Code)** field, enter a password.
Ensure that you make a note of the user name and password. The user name and password are required when creating a certificate for this server.

- f. In the **Confirm Password** field, re-enter the password.
 - g. In the **CN, Common name** field, enter the FQDN of Session Border Controller.
For example, Subject: CN=primary_sbc.acc.avaya.com,
CN=workspaces.acc.avaya.com, OU=SDP, O=AVAYA, C=US
 - h. In the first **DNS Name** field, enter the FQDN for the Avaya Workspaces cluster.
For example, DNS1: workspaces.acc.avaya.com.
 - i. In the **Token** field, select `P12 file`.
 - j. Click **Add**.
2. Create a keystore by performing the following steps:
- a. On the System Manager web console, click **Services > Security > Certificates > Authority**.
 - b. In the navigation pane, click **Public Web**.
 - c. On the EJBCA welcome page, in the navigation pane, click **Create Keystore**.
 - d. On the Keystore Enrollment page, enter the user name and password that you specified while creating the end entity.
 - e. Click **OK**.
 - f. Select the **Key Length** as 2048 bits.
 - g. Click **Enroll**.
 - h. Save the certificate file.

Creating a client profile for the Avaya Workspaces reverse proxy Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management > Client Profiles**.
3. On the Client Profiles page, click **Add**.
4. In the **Profile Name** field, type the name of the profile.
5. In the **Certificate** field, select the common client certificate that you created.
The certificate must include the internal interface IP that you need to specify in the **Connect IP** field while creating a reverse proxy service for Avaya Workspaces.
6. In the **Peer Verification** field, click **Required**.
7. In the **Peer Certificate Authority** field, use the CA that is used to sign your certificates.
8. In the **Verification Depth** field, type `1`.

9. Keep the default values in the other fields.
10. Click **Finish**.

Creating a server profile for the Avaya Workspaces reverse proxy

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management > Server Profiles**.
3. On the Server Profiles page, click **Add**.
4. In the **Profile Name** field, type the name of the profile.
5. In the **Certificate** field, select the common server certificate that you created.
The certificate must include the Avaya Workspaces cluster FQDN, because external clients use this FQDN to access Avaya Workspaces.
6. In the **Peer Verification** field, click **None**.
7. Keep the default values in the other fields.
8. Click **Finish**.

Extracting the certificate and private key in Session Border Controller

About this task

Use this procedure to extract the certificate and private key from the P12 file in Session Border Controller.

Procedure

1. Log in to Session Border Controller as root user by using an SSH client application, such as PuTTY.
2. Run the following command to extract the certificate from the P12 file:

```
openssl pkcs12 -in <filename>.p12 -out <filename>.pem -nokeys -clcerts
```
3. Run the following command to extract the private key from the P12 file:

```
openssl pkcs12 -in <filename>.p12 -out <filename>.key -nocerts
```

Installing the client and server certificates on Session Border Controller

About this task

Use this procedure to install the client and server certificates on Session Border Controller.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management > Certificates**.
3. On the Certificates page, click **Install**.
4. In the **Type** field, select `Certificate`.
5. In the **Name** field, type the name of the profile.
For example, `sbc_cert`.
6. In the **Certificate File** field, select the certificate that you extracted in Session Border Controller.
For example, `cert.pem`.
7. In the **Key** field, select **Upload Key File**.
8. Select the private key that you extracted in Session Border Controller.
9. In the **Key Passphrase** field, enter the password that you provided during private key generation.
10. Click **Upload File**.
11. Check the certificate to verify all details that you provided when creating the p12 file.
12. Click **Install**.

Chapter 14: Configuring reverse proxy for Avaya Workspaces

To enable remote access to Avaya Workspaces, you must first configure Avaya SBCE to allow calls from the public internet and then create a reverse proxy relay service for Avaya Workspaces.

To handle voice and video calls, Avaya Workspaces remote agents must use Avaya softphones or hardphones being logged in as remote workers. For more information about how to configure the remote worker feature, see *Administering Avaya Session Border Controller for Enterprise*.

Follow the instructions in this chapter for details.

Checklist for configuring reverse proxy for Avaya Workspaces

Use the following checklist to configure remote access to Avaya Workspaces:

No.	Task	Description	✓
1	Perform all the required prerequisite procedures.	See Prerequisites on page 176.	
2	Install and configure Avaya SBCE to enable calls from the public internet.	See Avaya Session Border Controller for Enterprise configuration on page 181.	
3	Document the Avaya Workspaces URLs that remote agents must have access to.	See the following procedures: <ul style="list-style-type: none">• Documentation of Avaya Workspaces configuration details on page 188	
4	Configure TLS client and server profiles.	See the following procedures: <ul style="list-style-type: none">• Configuring a TLS client profile on page 190• Configuring a TLS server profile on page 189	

Table continues...

No.	Task	Description	✓
5	Create a reverse proxy relay service for Avaya Workspaces.	See the following procedures: <ul style="list-style-type: none"> • Creating a reverse proxy relay service for Avaya Workspaces on page 191 	

Documentation of Avaya Workspaces configuration details

The reverse proxy determines which URL requests must be allowed and how the requests must flow into enterprise applications.

The reverse proxy is configured with a whitelist. Customers configure the whitelist for their deployment and it has all internal Avaya Workspaces URLs that all workers require to access the Avaya Workspaces functionality.

Consider the following:

- The EXT FW WAN IP value must be the same for all external server/cluster FQDNs, as externally, FQDNs for all back-end servers/clusters resolve to a single IP address on the external firewall.
- The SBC-EXT B1 IP must be the same for all servers/clusters, as the external firewall listens to incoming requests on ports 31380/31390 and routes these requests to the assigned B1 (external) interface on the Avaya SBCE using the NAT functionality.
- Based on the URL in the request, Avaya SBCE proxies the request through to an IP on the external (WAN) side of the internal firewall. Therefore, each back-end server/cluster is allocated to a unique IP:port combination on the external (WAN) side of the internal firewall.
- The internal firewall listens to incoming requests on all IP:port combinations on the external (WAN) side and routes these requests to the corresponding back-end Avaya Workspaces server/cluster using the NAT functionality.

Use the table below to document the required IP addresses used to configure the reverse proxy relay services for Avaya Workspaces.

Component	Your value	Description
External FQDN		External FQDN of the Avaya Workspaces cluster.
Internal Cluster IP		IP address of the Avaya Workspaces cluster.
Internal FW WAN IP		External IP address of the internal (WAN) firewall.

Table continues...

Component	Your value	Description
SBC-EXT B1 IP		IP address of the Avaya SBCE external (B1) interface.
Whitelisted URLs in request		All Avaya Workspaces URLs that remote agents must have access to. For example: /Login /GetNewToken /proxy /phonebookquery /attachment /services/OCPDataServices /services/CustomerManagement /services/CustomerJourneyService /services/UnifiedAgentController /services/Broadcast- UnifiedAgentController
EXT FW WAN IP		External IP address of the external (WAN) firewall.

Configuring a TLS server profile

About this task

The Avaya SBCE reverse proxy relay requires a TLS client profile and a TLS server profile. The server profile is for the interface facing the Internet.

Procedure

1. Log on to EMS web interface with administrator credentials.
2. From the Device list, select the SBCE.
3. In the navigation pane, click **TLS Management > Server Profiles**.
4. Click **Add**.

The EMS server display the New Profile window.

5. In the **Profile Name** field, type the name of the profile.

For example, `CC_Relay_Server`.

6. In the **Certificate** field, select the certificate for external communication.

The certificate must correspond to the external B1 interface used as the Listen IP for a reverse proxy relay.

7. In the **SNI Options** field, select **None**.
8. In the **Peer Certificate Authorities** field, select **None**.
9. Leave other settings as default.
10. Click **Next**.
11. Click **Finish**.

Configuring a TLS client profile

About this task

The Avaya SBCE reverse proxy relay requires a TLS client profile and a TLS server profile. The client profile is for the interface facing the internal Avaya Workspaces cluster.

Procedure

1. Log on to EMS web interface with administrator credentials.
2. From the Device list, select the SBCE.
3. In the navigation pane, click **TLS Management > Client Profiles**.
4. Click **Add**.

The EMS server display the New Profile window.

5. In the **Profile Name** field, type the name of the profile.

The profile name is `CC_Relay_Client`.

6. In the **Certificate** field, select the certificate for internal communication.

The certificate must correspond to the internal A1 interface used as the Connect IP for a reverse proxy relay.

7. In the **Peer Certificate Authorities** field, select the certificate for CA.

CA that signed the identity certs for the internal Avaya Workspaces cluster.

8. In the **Verification Depth** field, set the value to 1.
9. Leave other settings as default.
10. Click **Next**.
11. Click **Finish**.

Creating a reverse proxy relay service for Avaya Workspaces

About this task

A reverse proxy relay service is required for each server/cluster:port combination. Configure a relay for Avaya Workspaces.

Before you begin Procedure

1. Log on to EMS web interface with administrator credentials.
2. On the **Device** menu, click **SBCE**.
3. Navigate to **DMZ Services > Relay**.
The EMS server displays the Relay Services page.
4. On the Reverse Proxy tab, click **Add**.
EMS displays the Add Reverse Proxy Profile page.
5. In the **Service Name** field, type the reverse proxy profile name.
For example, `CC_Relay`.
6. Select the **Enabled** check box.
7. In the **Listen IP** field, select the B1 external network and then select the B1 IP address that is used for the relay.
8. In the **Listen Protocol** field, select **HTTP** or **HTTPS**.
9. In the **Listen Port** field, type 31380 for HTTP or 31390 for HTTPS.
10. In the **Listen TLS Profile** field, select the server TLS profile you created for the external B1 interface.
If the **Listen Protocol** is set to **HTTP** then this field is set to **None** automatically.
11. In the **Connect IP** field, select the A1 internal network and then select the A1 IP address that is used for the relay.
12. In the **Server Protocol** field, select **HTTP** or **HTTPS**.
13. In the **Server TLS Profile** field, select the client profile you created for the internal A1 interface.
If the **Server Protocol** is set to **HTTP** then this field is set to **None** automatically.
14. In the **Reverse Proxy Policy Profile**, select the reverse proxy policy that you created.
15. In **Server Addresses**, type the internal firewall IP address assigned to the Avaya Workspaces cluster and a corresponding port number.
Use port number 31390 if security is enabled and port number 31380 if security is disabled.

16. In **Whitelisted URL**, type all internal Avaya Workspaces URLs that remote agents must have access to.
17. Click **Finish**.

Part 5: First phone call and first email

Chapter 15: Agent Desktop

Agent Desktop is a single-interface client application used to interact with customers. You can use it to respond to customer contacts through a variety of media, including phone, outbound contacts, email, Web communication, fax, scanned documents, and Short Message Service (SMS) text messages.

Agent Desktop provides automation for customer responses to eliminate repetitive actions, such as typing a common response in an email message.

*** Note:**

Agents must use Agent Desktop to handle voice and multimedia contacts. Avaya Contact Center Select does not support telephone-only operations for voice agents.

Agent Desktop User Interface

Use Agent Desktop to handle voice, email, Web communications, SMS text message, voice mail, fax, and scanned documents contacts. Use Agent Desktop in the following situations:

- to handle voice contacts in a voice-only contact solution
- to handle voice contacts, email messages, or Web communications contacts in a voice and multimedia contact solution

This chapter describes the main user interface of the Agent Desktop application. There are three main sections to the Agent Desktop user interface:

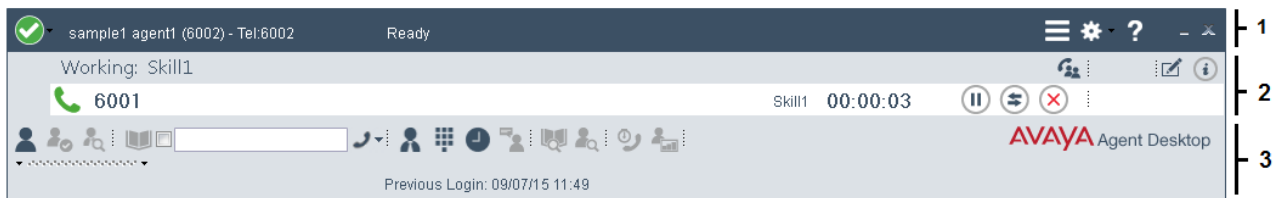


Figure 7: Example of Agent Desktop layout

1	Top bar on page 195
2	Work list window on page 196
3	Action bar on page 197

Agent Desktop also provides other controls and menus that are explained in the following chapters.

Work Item paradigm

The main Agent Desktop user interface is based on a work item paradigm. Each agent-to-customer interaction is a work item. Work items appear on the Agent Desktop work list.

The work list consists of work items and control buttons corresponding to the work item. The controls and functions change depending on the work list window behavior. When a new contact arrives, Agent Desktop adds the new contact as a work item to the work list.

Top bar

The Top bar appears at the top of the Agent Desktop window. The Top bar provides the system status and main controls to operate the Agent Desktop.



Figure 8: Example of Top bar layout

The agent status icon appears on the top left corner of the Agent Desktop Top bar. The Top bar also displays the agent status, agent name, agent login ID, and dialable number of the agent.

The Top bar has the following icons:

Table 3: Top bar icons

Icon	Name	Description
	Agent status	Select agent status.
	Terminal Actions	Access Emergency.
	User preferences	Access user preferences, open the Dashboard, and change work item display settings.
	Help	Access help information.

Use the Terminal Action menu to perform the following tasks:

Table 4: Terminal Action Menu

Command	Description
Emergency	Immediately connect with your supervisor in case of emergency.

Work list window

The work list window contains work items and control buttons corresponding to the work item. The controls and functions change depending on the information in the work list window. The top-right corner of the work list window has work item controls. These controls are common to all work items on the work list. When a new contact arrives, Agent Desktop adds the new contact as a work item to the work list.

The following figure shows the work list windows and controls.

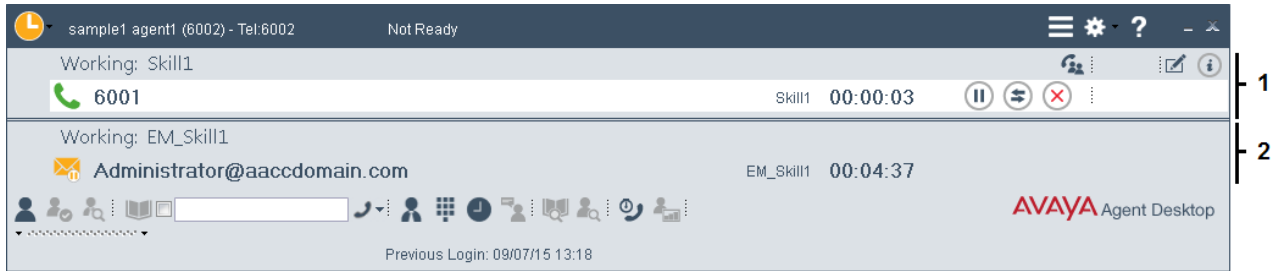


Figure 9: Example of work list layout

The illustrated work list shows two work items:

1	A voice call work item, at the top of the work list.
2	An email work item, at the bottom of the work list.

- A work item is a collection of interactions with a customer, another agent, a supervisor, or an expert.
- A work list is a collection of work items. When you receive a new contact, it is added to the work list so that you can monitor your current contacts. When you finish with the contact, or reject the contact, the work item is removed from the list.

























Work item controls:

Each work item has a number of contact-related controls. These controls change depending on the work list window behavior and contact type.

Table 5: Examples of work item controls

Voice	Email	WC	SMS	Voice mail	Fax	Name	Description
						Accept	Accept the work item.
						Release	Release or reject the work item.
						Hold	Place the work item on hold.

Table continues...

Voice	Email	WC	SMS	Voice mail	Fax	Name	Description
						Transfer	Transfer the work item contact.
						Conference/Join	Conference the work item. Or join two work items.
						Activity code	Set the work item activity code.
						Work item details	Read work items details.

Only appropriate controls are displayed on work items. Voice-related controls are displayed on voice work items. Email-related controls are displayed on email work items.

Action bar

The Action bar contains global controls to create a new work item, to search contacts, and to open secondary windows. The Action bar is located at the bottom of the Agent Desktop window.



Figure 10: Example of Action bar layout

Use the Action bar at the bottom of the main interface to make new contacts. New voice or email contacts are collectively called new work in the Work Item Paradigm.

Table 6: Action bar commands







Icon	Name	Description
	Customer Details	View customer details.
	Contacts Presence	Contact presence.
	Observe	Listen in or participate in agent-customer calls or chat sessions. (Used by agent-supervisors only)
	Phonebook	Contact agents through the LDAP agent contact directory.
	Originate Call	Start a new work item.
	Supervisor	Call your supervisor.

Table continues...

Icon	Name	Description
	DTMF	Generate Dual-tone Multi-frequency (DTMF) tones.
	Contact Search	Search for contacts.
	Customer Search	Search for customers.
	Schedule Callback	Schedule a callback.
	Agent Statistics	Display the agent statistics scroll bar.

Email User Interface

Use Agent Desktop to handle incoming email messages. You can also use Agent Desktop to create a new email message.

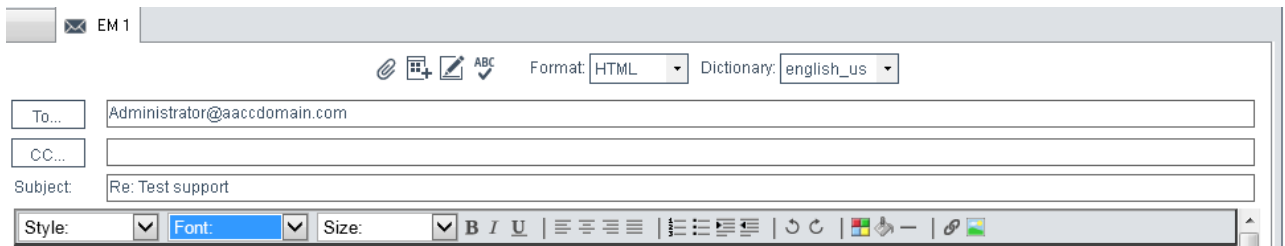


Figure 11: Example of email toolbar





The Agent Desktop email editor offers improved email editing, formatting feature buttons, and management in HTML format email messages.

The following table describes the email feature buttons:

Table 7: Email editing and formatting controls

Control	Name of the Control	Function
	Bold	Bold the selected text
	Italic	Italicize the selected text
	Underline	Underline the selected text
	Left	Align text with left margin
	Center	Center text

Table continues...

Control	Name of the Control	Function
	Right	Align text with right margin
	Justify	Justify text
	Numbers	Numbered list items
	Bullets	Bulleted list items
	Indent	Indent selected text
	Outdent	Outdent selected text
	Undo	Undo last change
	Redo	Redo the last change
	Color	Change color of selected text
	Link	Insert a hyperlink
	Image	Insert an inline image
	Insert a file	Insert an email attachment
	SpellCheck	Spell check the email message
	Insert Signature	Insert a signature to the email message
	Insert a Template	Email templates
	Rule	Adds a continuous line under the selected location
	Highlight	Highlights selected text with a color chosen from the color palette

Installing Agent Desktop software using ClickOnce

Before you begin

- Ensure the client computer meets the hardware and networking requirements for Agent Desktop software. For more information about Agent Desktop requirements, see *Avaya Contact Center Select Solution Description*.
- Ensure the client computer meets the Operating System requirements for Agent Desktop software. For more information about Agent Desktop requirements, see *Avaya Contact Center Select Solution Description*.

About this task

Install Agent Desktop software to handle Avaya Contact Center Select customer contacts.

Procedure

1. In Windows Explorer, Internet Explorer or Microsoft Edge, type the HTTP address (URL) provided by your system administrator.

The URL format is:

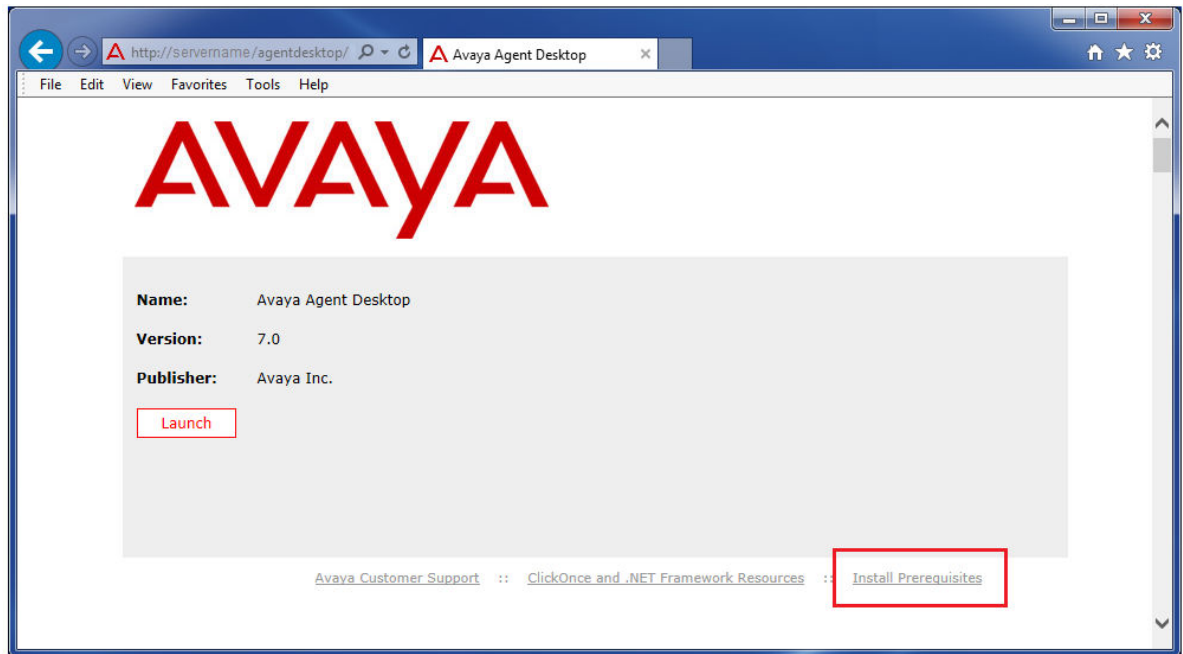
`http://<ContactCenterServerName>/agentdesktop`

Where <ContactCenterServerName> is the Avaya Contact Center Select server name.

*** Note:**

The Agent Desktop installer does not use a secure HTTPS connection, even if Web Services security is turned on.

2. Click **Install Prerequisites** and follow the on screen instructions to install the .NET and operating system components required to run Agent Desktop software.



3. Click **Launch** to download and install the most recent version of Agent Desktop software.

Logging on to Agent Desktop

About this task

Log on to Agent Desktop and change into the ready state to handle customer contacts.

To support rapid and easy deployment, Avaya Contact Center Select provides some default users and supervisors.

The default sample supervisor “6001” can handle both voice contacts and email messages. To test both voice contacts and email messages, log on as supervisor “6001” and use the default password.

The default sample user “6002” can handle only voice contacts. To test voice contacts, log on as user “6002” and use the default password.

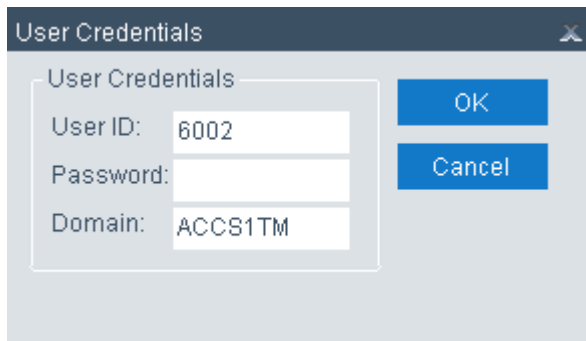
The default users and supervisors all have the same default password. This default password is configured on the *Sample Data* tab of the Avaya Contact Center Select Ignition Wizard during deployment.

*** Note:**

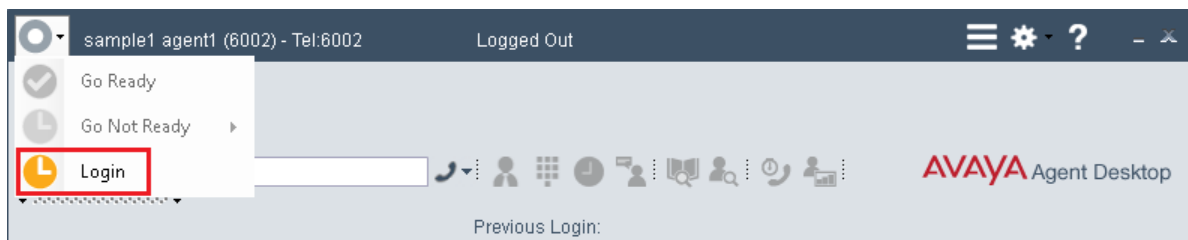
You must be logged on to the desktop phone before you log on to Agent Desktop.

Procedure

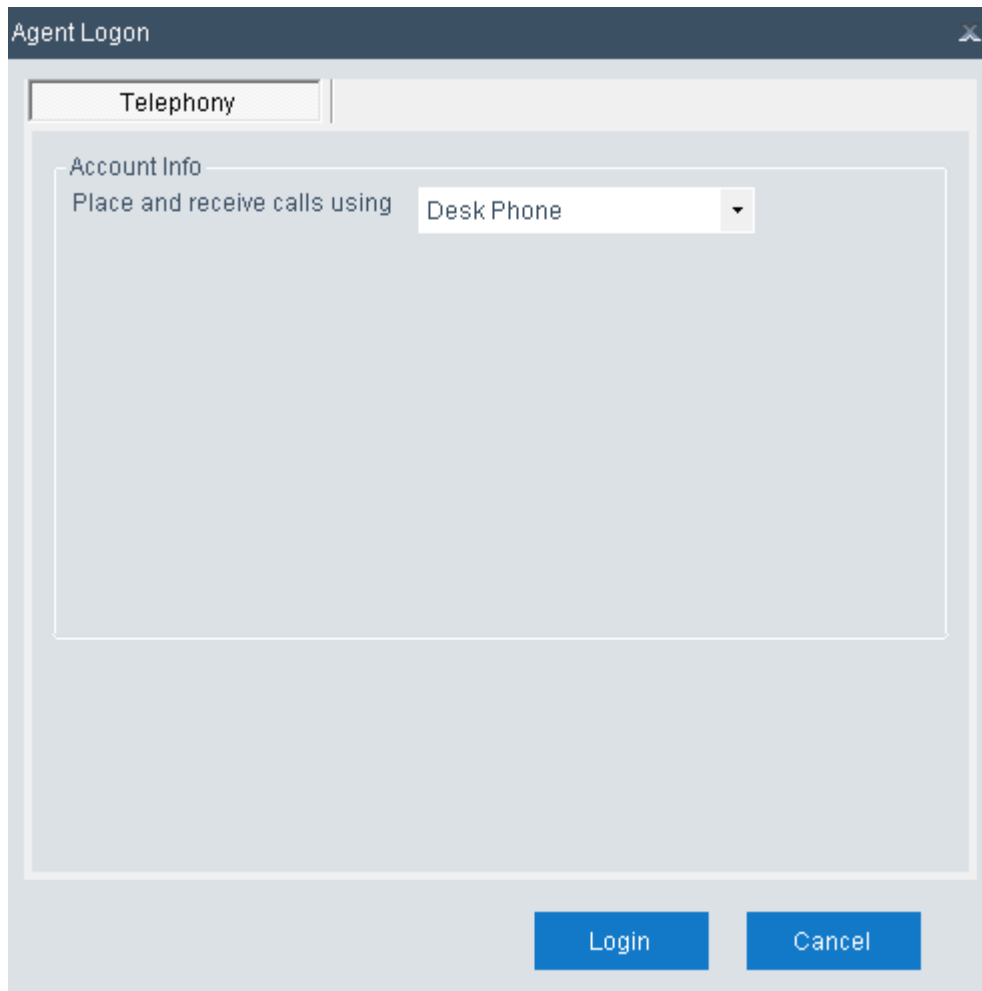
1. On the Agent Desktop client computer, click **Start > All Programs > Avaya > Avaya Agent Desktop**.
2. On the **User Credentials** window, in the **User ID** box, type the agent user ID. For example, type 6002.



3. In the **Password** box, type the password for the agent.
4. In the **Domain** box, type the host name of the Avaya Contact Center Select server.
5. Click **OK**.
6. On the Agent Desktop Top bar, from the **Status** list, select **Login**.

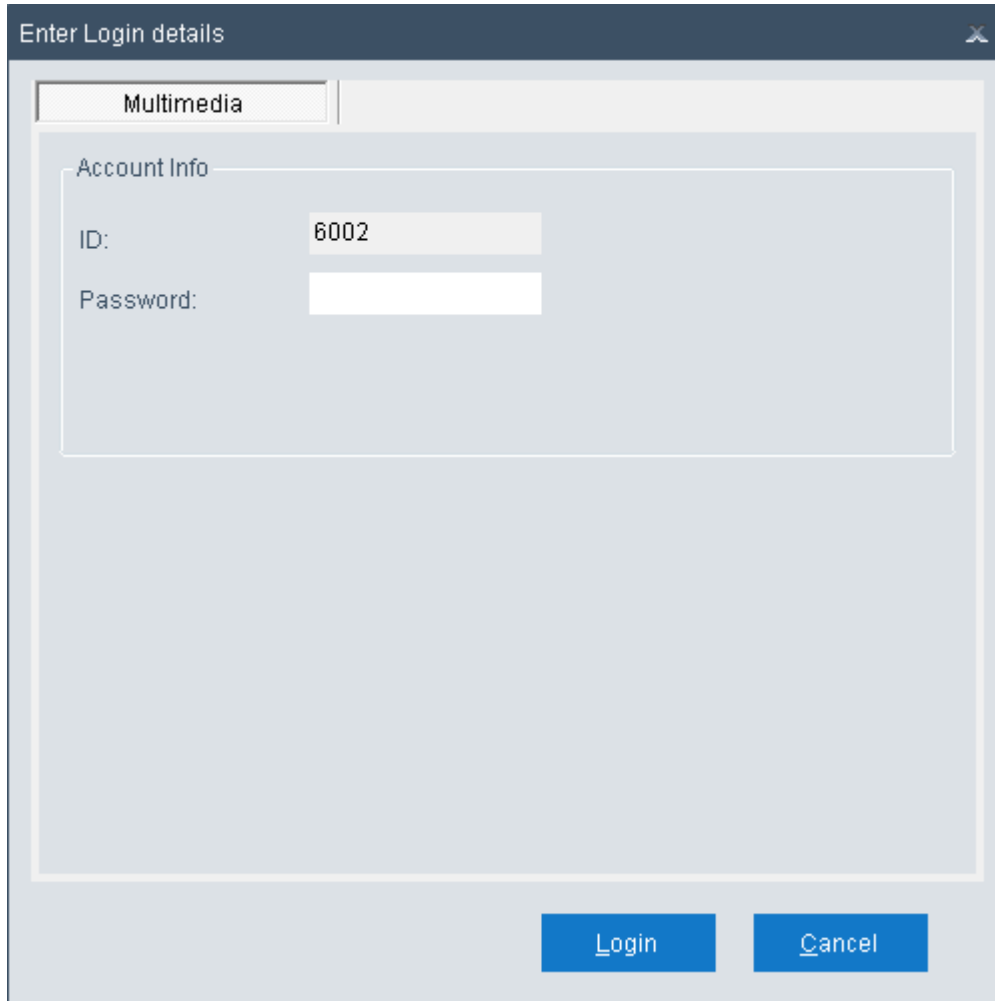


7. On the **Agent Logon** window, click **Login**.



8. If the user is configured to handle multimedia contacts (such as email), on the **Multimedia** tab, type the user **ID** and **Password** and click **Login**. Use the same user ID and password as above.

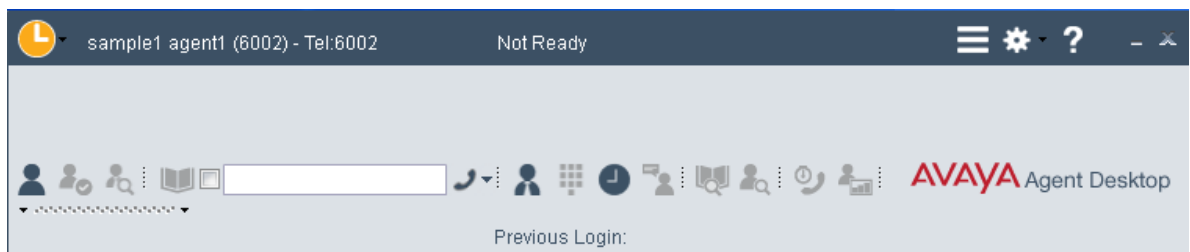
For example:



9. If you logged on with an account configured for multimedia, Agent Desktop prompts you to change the multimedia password.

You must change the Multimedia password to continue.

Agent Desktop completes the logon and the status icon changes to Not Ready.



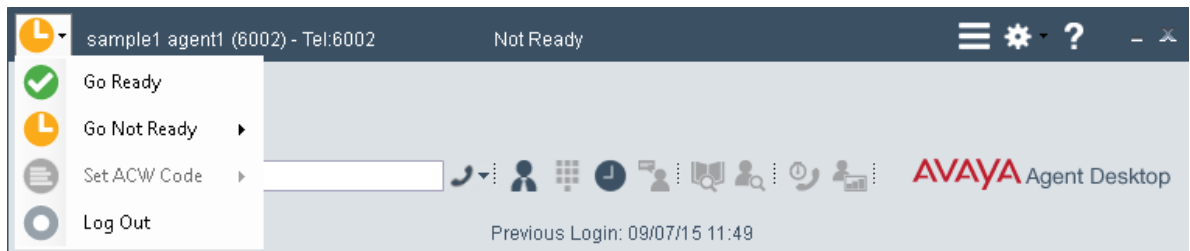
Changing your status to Ready

About this task

Change your status to Ready when you are available to create and receive contacts.

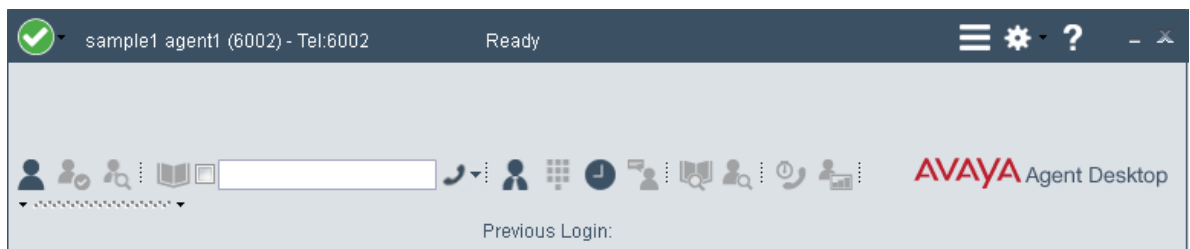
Procedure

1. On the Agent Desktop Top bar menu, click the **Status** icon.



2. Select **Go Ready** to create or receive both voice and multimedia contacts.

The status icon changes to green.



Making a test phone call to the contact center

Before you begin

- Ensure an Avaya Contact Center Select agent is logged on to Agent Desktop and is in the ready state.

About this task

Make a test phone call to the Avaya Contact Center Select CDN (Route Point).

Procedure

1. Using an IP Office phone, dial the Avaya Contact Center Select CDN (Route Point) phone number. For example, dial 3000.
2. Listen for a ringback tone.
3. Listen for the “Welcome to the Contact Center” announcement.

4. Listen for the following voice prompt menu:
 - “Press 1 to speak to an agent at the help desk.”
 - “Press 2 to speak to an agent in the support center.”
 - “Press 3 to Enter your pin number or any eight digits of your choosing.”
 - “Press 4 to leave a voice mail.”
 - “Press * to repeat this menu.”
5. To make a test phone call and speak with an agent, press button 1 on your phone.
6. Listen for another ringback tone as your call is routed to an available Avaya Contact Center Select agent.
7. Wait for the call to be answered by an agent.

Accepting a call

Before you begin

- Ensure that you have set your status to **Go Ready**.
- Ensure that you are assigned to a skillset for handling telephone calls.

About this task

Accept and work with telephone calls. The relevant work item controls become active and the call timer appears on the work item.

If your administrator has configured your Contact Center to run in the Call Force Delay mode, you must handle all contacts presented to you.

Procedure

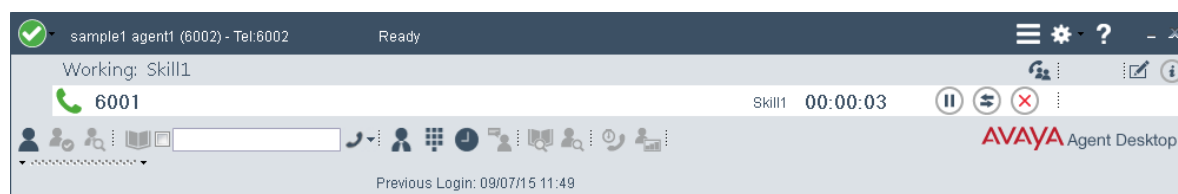
1. On Agent Desktop, select the new **Alerting** work item.

Example of an alerting contact center Route Point call:



2. Click the **Accept** work item control.

Example of an answered contact center Route Point call:



The agent can now speak with the customer.

Entering an Activity code

About this task

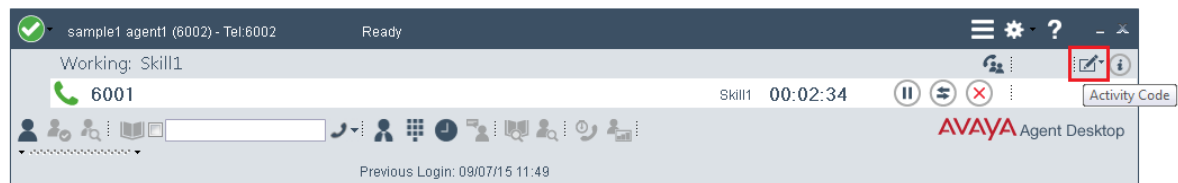
You can enter one or more Activity codes during calls by using the Agent Desktop Top bar activity inline command. Activity codes provide a method to track the time that agents spend on various types of calls. For example, you can enter a Sales activity code in Agent Desktop during a sales-related call.

Your supervisor or system administrator configures Activity codes. Administrators define Activity codes in Contact Center Manager Server. Activity codes can be alphanumeric. Agent Desktop displays the Activity codes list.

Agent Desktop displays the **Activity Code** box on the work item based on your Contact Center configuration. Administrators can configure activity codes that correspond to a contact type and a skillset. Therefore, Activity codes are filtered on a contact type and skillset basis. For example, if you are handling email contacts, Agent Desktop populates the **Activity Code** list with activity codes that correspond to the email contact type and skillset.

Procedure

1. Select the work item.
2. Click the **Activity Code** work item inline command.
3. From the **Select or type an Activity Code** drop-down list, select or type the activity code.



Ending a call

About this task

End a call when a call is completed. If your status was Ready before the call, your status is automatically set to Ready, when you terminate the call. If you require time to perform call wrap-up tasks, before you accept another call, select **Set ACW Code** and enter the After Call Work Item (ACW) code in the **Code** field of the Top bar. If you require to change your status to Not Ready and enter a Not Ready Reason Code in the **Code** field of the Top bar. The administrator defines Not Ready Reason and ACW codes.

Procedure

On the work item, click **Release**.

Making a call

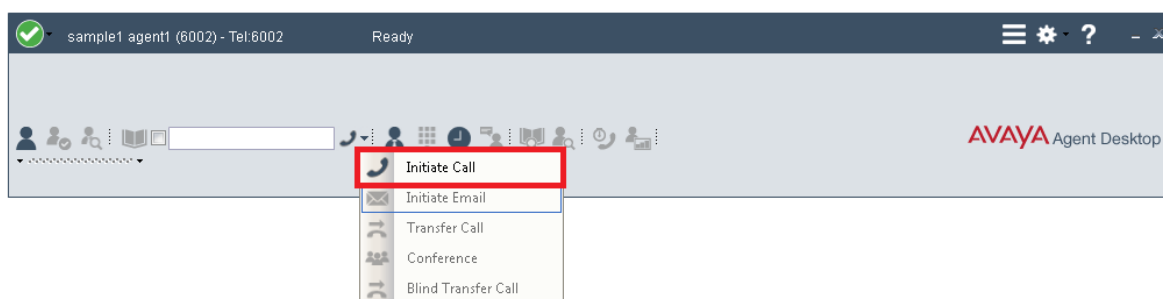
About this task

Make a call using Agent Desktop. Ensure that you follow the steps based on the type of phone number you want to call:

- the default phone number
- a new external phone number
- a new internal phone number

Procedure

1. On the Agent Desktop Action bar menu, click **Initiate Call**.



2. In the **Initiate Call** text box, enter the phone number to dial.
3. Click **Initiate Call** again.

The phone number is dialed. A new work item is added to the work list and the call timer on the work item starts to increment.

4. Click **Release** when you complete the call.

Sending a test email message to the contact center

Before you begin

- Know the name of a mailbox monitored by Avaya Contact Center Select.

About this task

Send a test email message to Avaya Contact Center Select.

Procedure

1. Create an email message.
2. Send the email message to the mailbox monitored by Avaya Contact Center Select.
3. Avaya Contact Center Select processes the email. You might receive an automated acknowledgement of your email before an Avaya Contact Center Select agent responds.

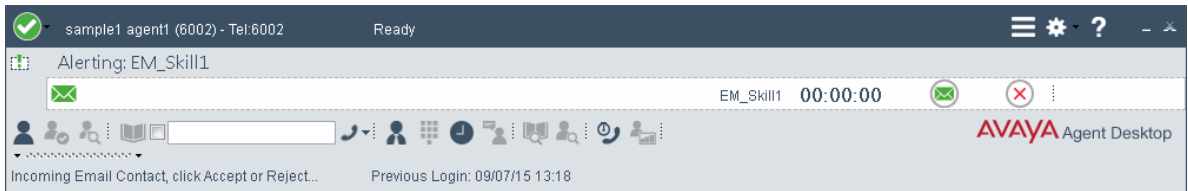
Accepting an incoming email message

About this task

Accept an incoming email message, when you are ready to receive the customer's email, display customer details and begin contact with a customer. The Agent Desktop displays the customer details and the call timer appears on the work item. The new incoming email message is presented as a new work item in the Work List window.

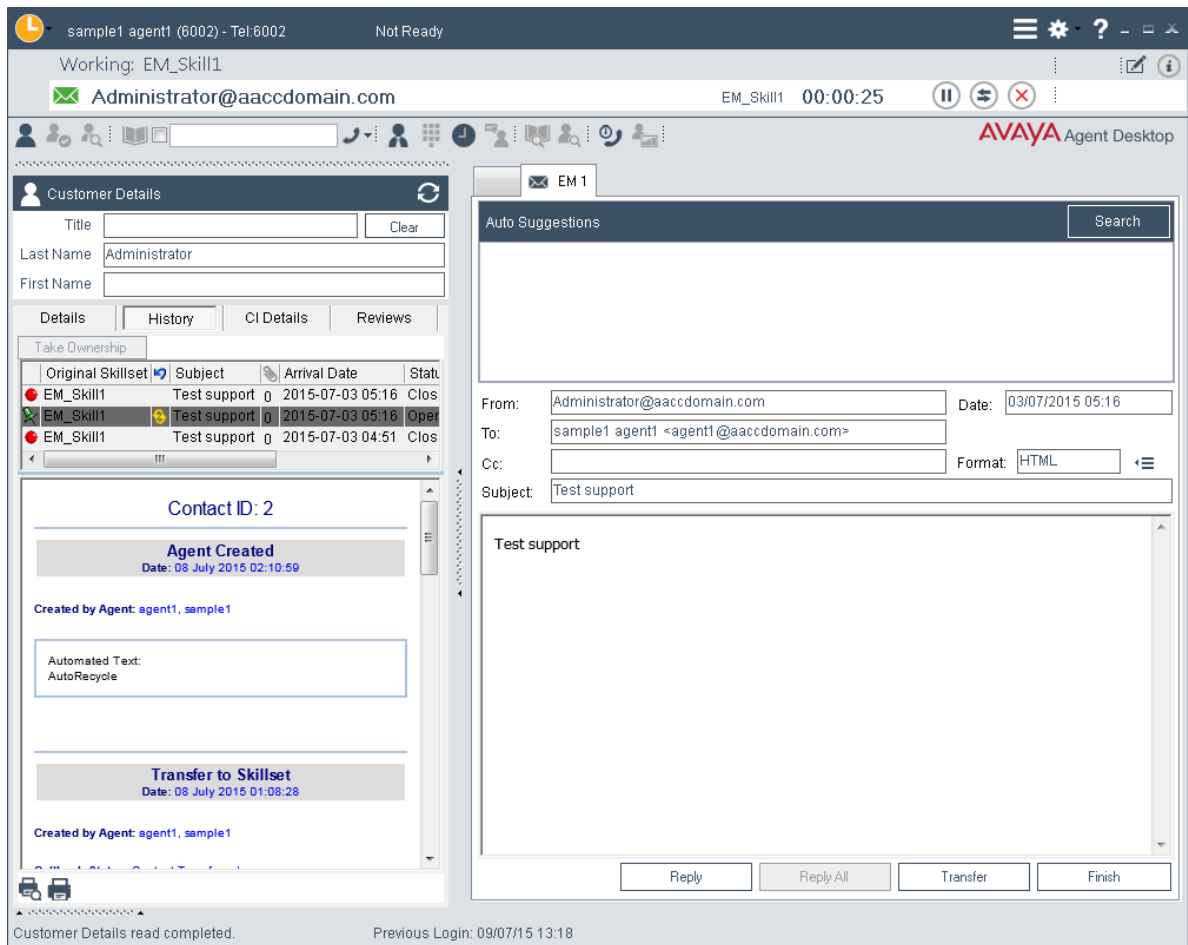
Procedure

1. The incoming email message appears on the Agent Desktop Work List window.



2. On the Agent Desktop, click **Accept**.

The email message opens in the E-mail Display panel.



The customer details associated with the email message appears in the bottom left-hand corner of the Customer Details panel.

Replying to an email message

Before you begin

- Accept an email contact.

About this task

Reply to an email message when a customer sends an email message to the Contact Center requesting a response. Create a response to a customer in the same format as the original request.

You can use several features (present in the following list) in the Agent Desktop interface to create your email response in HTML or plain text:

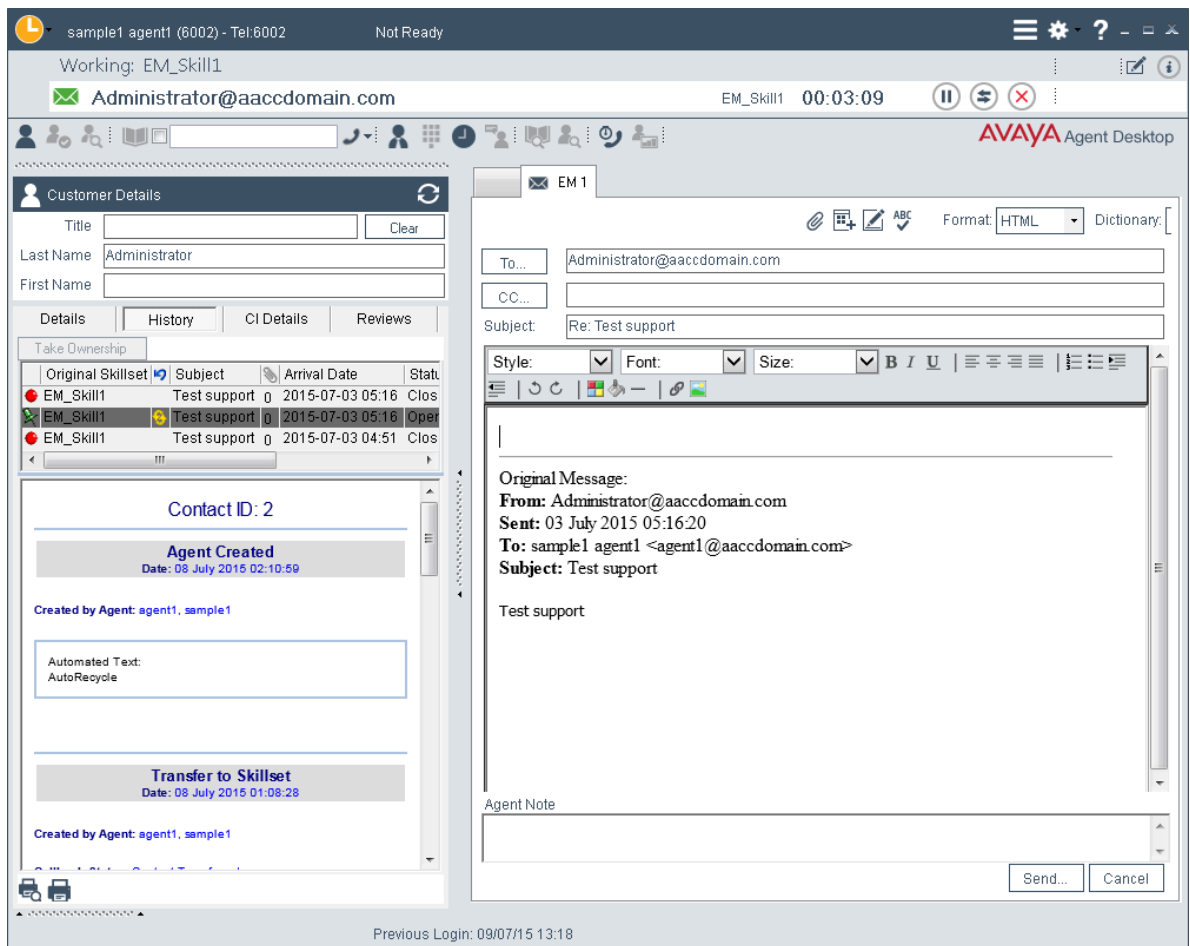
- Auto suggestions

- the address book
- one or more response templates
- an automatic signature
- an attached file
- the spelling checker

You can also add a comment to an email message in the **Agent Note** box as a reference for later communications with the customer. The customer does not see the information present in the **Agent Note** box.

Procedure

1. On the Agent Desktop, in the Email window, click **Reply**.



2. In the E-mail Response window, accept the default **To** email address. The default email address is the address from which the message was sent.

Or

Click **To** to add an email address of the customer, which is other than the default email address.

Or

Click **Cc** to add other email addresses from the corporate address book or multimedia database.

3. In the **Subject** box, either accept the subject currently displayed or edit the subject.
4. Add text to the reply using one or both of the following methods:
 - Type the message text.
 - Add a template response.
5. If you use the HTML format for creating the email message, and you want to make the text bold, underline, or italics, select the text, and click the appropriate button to apply formatting.

You cannot format a plain text email message.

6. To change the text size, select the text and click the up arrow to increase the font size, or click the down arrow to decrease the font size.
7. To perform a spell check, click the **SpellCheck** icon.
8. To insert an automatic signature to the email message, click the **Insert Signature** icon.
9. To add an attachment to the email response, click **Insert a file**.
10. In the **Agent Note** box, type additional information about the contact or the customer, if required.

Only agents and supervisors can view the information in the **Agent Note** box.

11. Click **Send**.
12. Close the contact.

If required, select a reason for closing the contact.

Logging off from Agent Desktop

Before you begin

- Ensure that you do not have a contact open. If a contact is open, you must close the contacts before you log off of the application.

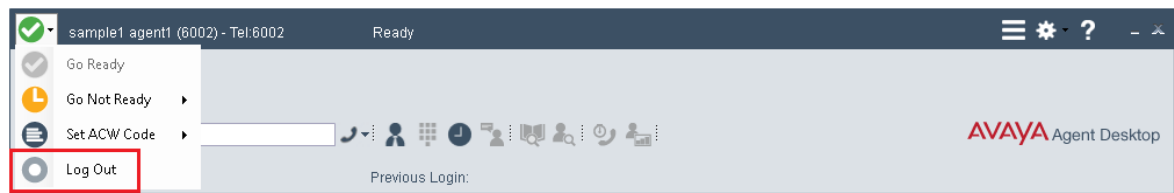
About this task

Log off from Agent Desktop when you are ready to exit the application.

Procedure

1. On the Agent Desktop Top bar menu, click the **Status** icon.

2. Click **Log Out**.



Agent Desktop logs you off. The status icon changes color and the Top bar displays the Logged Out status.

Part 6: Maintenance

Chapter 16: Maintenance procedures

This section describes how to maintain the Avaya Contact Center Select software and server. You must maintain Avaya Contact Center Select to protect against data loss and to ensure that you are using the most recent software.

Database maintenance

Perform an immediate backup of the Avaya Contact Center Select databases to save the current data. It is important to complete this procedure after you complete your installation or when any significant change occurs in the database, so that you can restore the database easily. Perform backups during low traffic periods. Avaya Contact Center Select services are not shut down during backups. Back up the databases to a secure network location. Schedule regular backups of the Avaya Contact Center Select databases to ensure resiliency against media failure or data loss.

Contact Center Software patches

Apply the most recent Avaya Contact Center Select patches to ensure that you have the most recent version of the application software and to resolve software issues.

Install the latest operating system service packs that are supported for Avaya Contact Center Select. You must download the latest supported operating system service pack from the Avaya hotfixes list to ensure your Avaya Contact Center Select server software functions correctly with the supported operating system patches.

Adding a server to a domain

Before you begin

- Ensure that you have domain administrator privileges, or ask the Domain Administrator to assign you a domain user account for remote access.
- On the server, configure a preferred Domain Name System (DNS) server on the Network Interface Card (NIC).

About this task

Add the server to an existing domain.

Note:

Add the server to a Windows domain before installing Contact Center software. When joining the domain, ensure the server time and domain controller time are synchronized to the same time.

Ask your System Administrator to add a Domain Name System (DNS) static entry for this server. Each Contact Center server in a domain requires a DNS static entry.

Procedure

1. Log on to the server.
2. On the **Start** screen, select **Administrative Tools > Server Manager**.
3. In the left pane, select **Local Server**.
4. In the right pane, in the **Properties** section, double-click on the **Domain** value.
The **System Properties** dialog box appears.
5. In the **System Properties** dialog box, click the **Computer Name** tab.
6. Click **Change**.
7. In the **Member of** section, click the **Domain** option.
8. Type the domain name (you must provide the fully qualified domain name, which includes the prefix and suffix).
9. Click **OK**.
10. Type the domain administrator **User name** and **Password**.
11. Click **OK**.
12. Restart the server when you are prompted to do so.

Backing up the Contact Center databases

About this task

Perform an immediate backup of the Contact Center server databases to save the current data. Perform a scheduled backup to maintain snapshots of data for emergency purposes. For more information about scheduled backups, see [Scheduling a backup of the Contact Center server databases](#) on page 218.

It is important to complete this procedure after you complete your installation or when any significant change occurs in the database, so that you can restore the database easily if required.

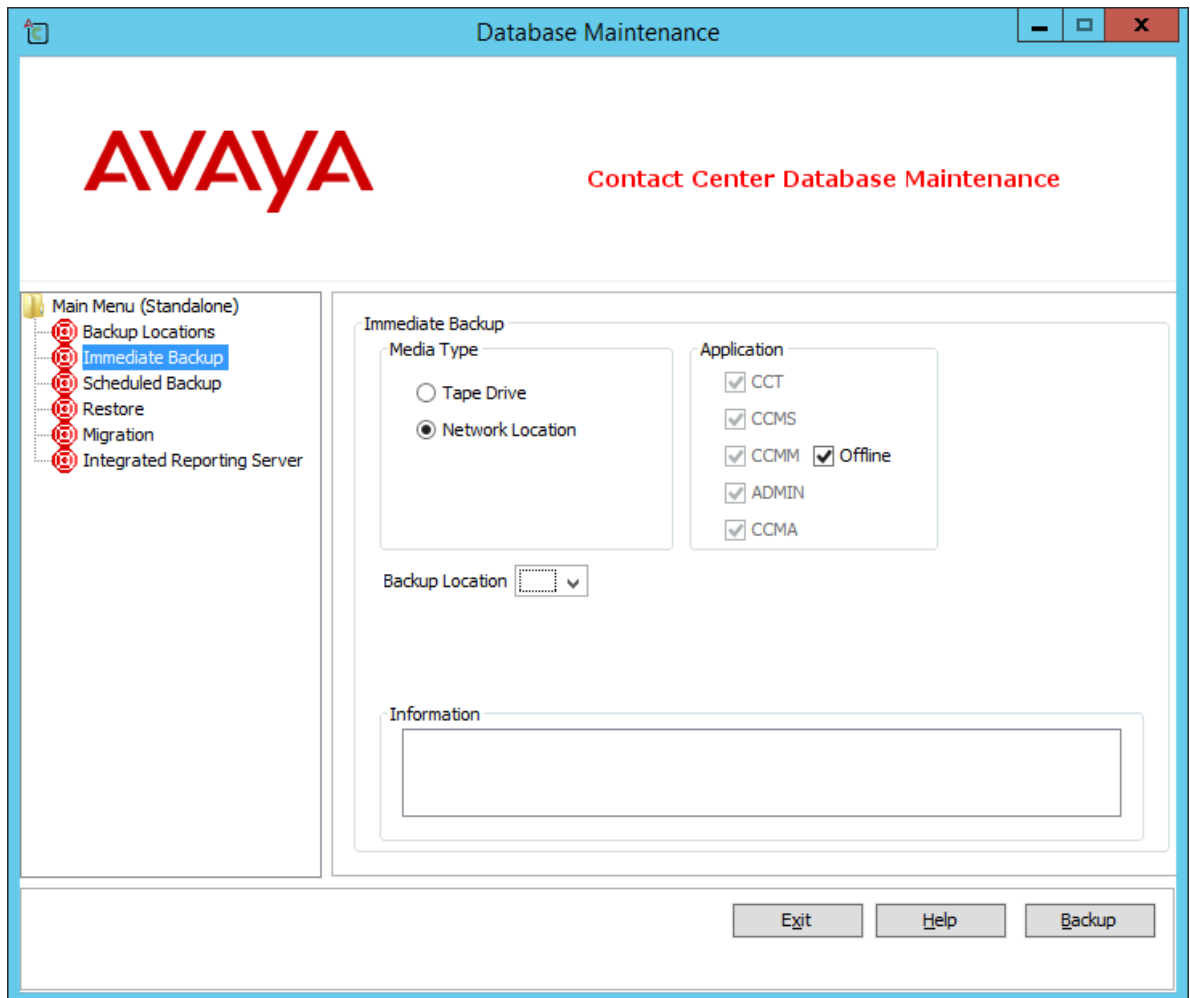
Perform backups during low traffic volume periods.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Database Maintenance**.
2. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
3. In the right pane, click **Create**.

Maintenance procedures

4. From the **Drive Letter** list, select the network drive on which to store the Contact Center database.
5. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name \Folder\Backup Location.
6. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
7. In the **Password** box, type the user password.
8. Click **Save**.
9. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.



10. In the **Media Type** section, select **Network Location**.
11. From the **Backup Location** list, select the network drive on which to store the backup.
12. Click **Backup**.

13. Click **Yes**, to continue with the backup.

The database is backed-up.

14. Click **Exit**.

Creating a backup location for scheduled backups

Before you begin

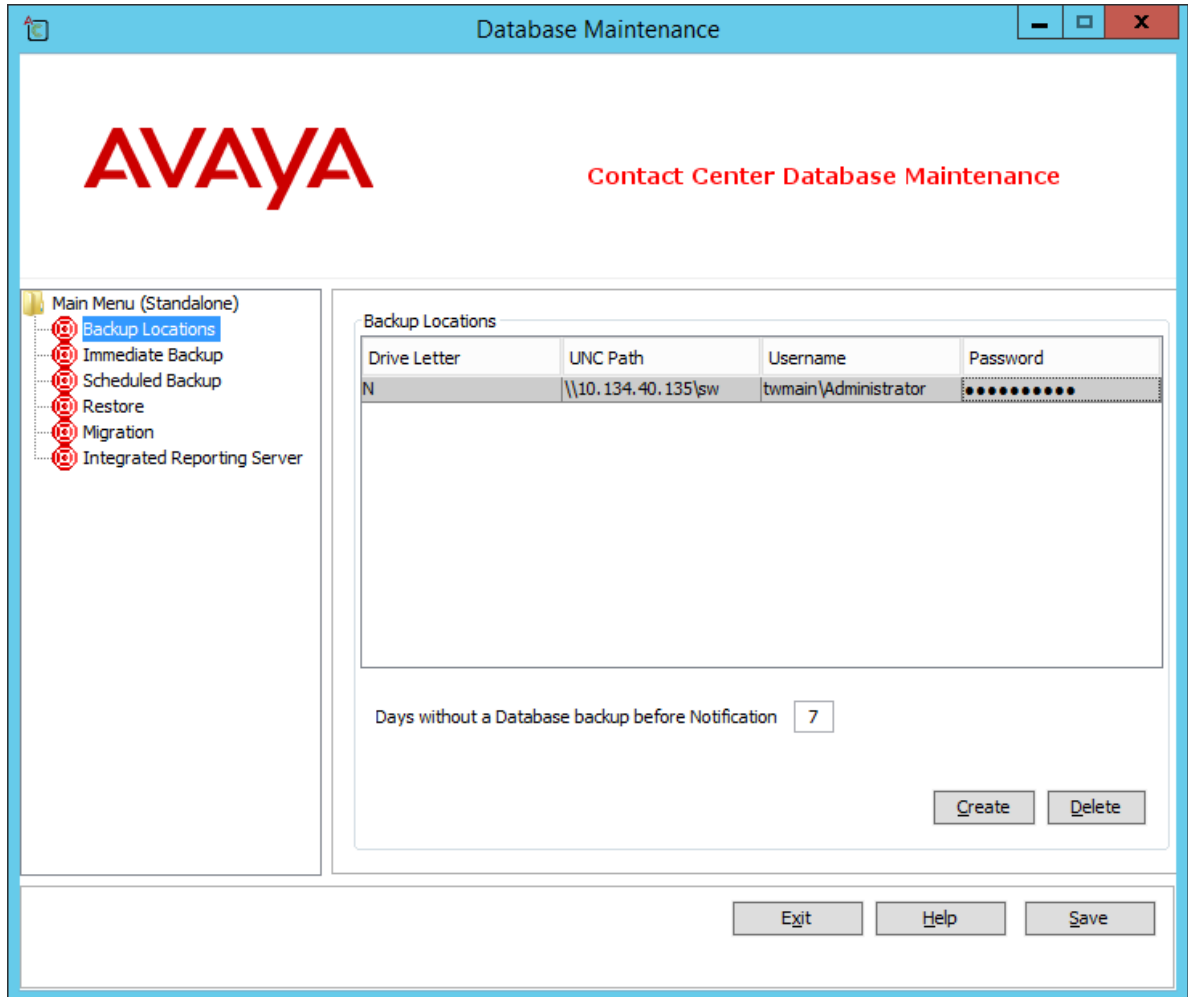
- Ensure that you log on with a user account with full permissions to access the location where you store the database backups.

About this task

Create a backup location on your network with the correct access permissions to ensure that you have a designated location for the scheduled backups.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Database Maintenance**.
2. In the Database Maintenance dialog box, click **Backup Locations**.
3. In the right pane, click **Create**.
4. From the **Drive Letter** list, select a drive letter.
5. In the **UNC Path** text box, type the location to which to back up the database.
6. In the **Username** box, type the user name used to log on to the server specified in the UNC Path box in the format Computer Name\Account Name.
7. In the **Password** box, type the Windows password.
8. Click **Save**.



Scheduling a backup of the Contact Center server databases

Before you begin

- Create a backup location. For more information, see [Creating a backup location for scheduled backups](#) on page 217.

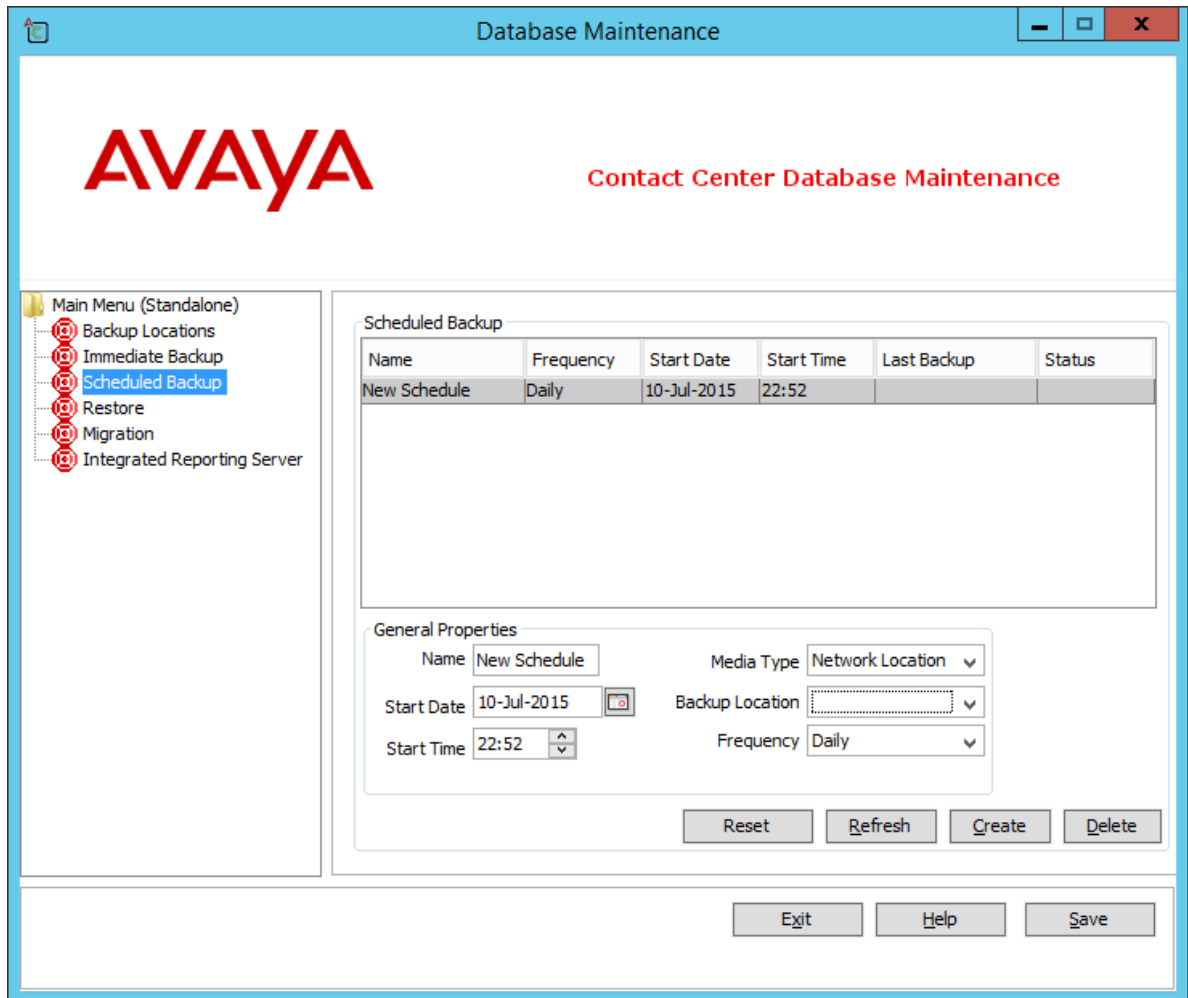
About this task

Schedule a backup of the Contact Center server databases to save the data regularly. Perform a scheduled backup to maintain snapshots of data for emergency purposes.

Perform backups during low traffic volume periods.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Database Maintenance**.
2. In the Database Maintenance dialog box, in the left pane, click **Scheduled Backup**.



3. In the right pane, click **Create**.
4. Under **General Properties**, in the **Name** box, type a name for the scheduled backup.
5. From the **Media Type** list, select **Network Location**.
6. In the **Start Date** box, type the date on which to begin scheduled backups.

OR

Click the calendar icon and select a date on which to begin scheduled backups.

7. In the **Start Time** box, select the time to start the backup.
8. From the **Backup Location** list, select a drive to store the backup.
9. From the **Frequency** list, select the frequency of the backup.

Maintenance procedures

10. Click **Save**.
11. In the confirm dialog, click **OK**.
12. Click **Exit** to close the Database Maintenance utility.

Downloading the latest product documentation

About this task

Download the latest product documentation to ensure that you have the most recent updates. Updates in the documentation accurately reflect the latest software changes.

Procedure

1. Log on to the Avaya website at <http://support.avaya.com>.
2. Compare the versions of the product documentation on the site with the versions you have.
3. If the version number on www.avaya.com is higher than the version number on the documentation you have, download the latest version of the document.
4. Review the Avaya website for release notes and readme files.

Installing the most recent supported operating system service packs

Before you begin

- Access the Avaya hotfixes list on the website <http://support.avaya.com>.
- Review the specifications on operating system service updates in *Avaya Contact Center Select Solution Description*.

About this task

Avaya recommends that you install the most recent supported operating system service packs. You must download the supported operating system service pack from the Avaya hotfixes list to ensure your Contact Center server software functions correctly with the supported operating system patches.

Procedure

1. Review the Contact Center Service Packs Compatibility and Security Hotfixes Applicability List to determine the most recent Contact Center supported patches or service packs.
2. Download the appropriate Microsoft Windows Server patches for the Contact Center software installed on this server.

3. Install the most recent Microsoft Windows Server service pack that is validated with Contact Center by following the Microsoft Installation instructions.

Verifying if installed patches are up-to-date

Before you begin

- Look up the latest patches and upgrades for your Contact Center server at <http://support.avaya.com>.

About this task

Verify if installed patches are up-to-date by using the Contact Center Update Manager to view available patches and to verify the patches that are already installed on the server. Use the Update Manager to view the readme files associated with each patch.

Procedure

1. Log on to the Contact Center server where you want to view available patches,
2. On the **Apps** screen, in the **Avaya** section, select **Update Manager**.
3. Compare the most recent update name in the Update Manager with the latest patches listed on the Avaya website.

Downloading the most recent Contact Center patches to the server

Before you begin

- Ensure that you use an account with administrator privileges on your server.

About this task

Download the most recent Contact Center patches to the server from <http://support.avaya.com> to ensure that you have the most current software.

You can also download the most recent Avaya Workspaces patches to the server. For more information about downloading the most recent Avaya Workspaces patches to the server, read the *Using Avaya Workspaces for AACC and ACCS* guide.

Procedure

1. Log on to the server using an account with administrator privileges.
2. If a new service pack .msi file exists on <http://support.avaya.com>, download it and save it on the Contact Center server.

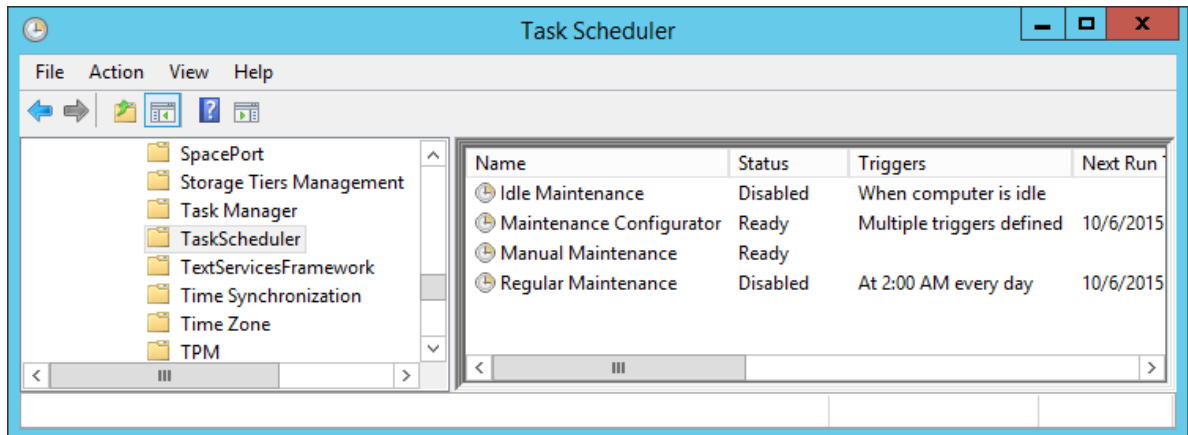
Disabling Windows Server Automatic Maintenance

About this task

Disable Windows Server Automatic Maintenance while updating Contact Center software. Windows Server Automatic Maintenance can occasionally interfere with the real-time requirements for Contact Center. You must therefore temporarily disable Automatic Maintenance to update Contact Center software. You re-enable Automatic Maintenance after updating Contact Center.

Procedure

1. Log on to the Contact Center server as Administrator.
2. On the **Desktop** screen, right-click **Start** and select **Run**.
3. In the **Run** text box, type `Taskschd.msc`.
4. Click **OK**.
5. On the **Task Scheduler** window, in the left pane, select **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
6. In the **Name** column, right-click **Idle Maintenance** and select **Disable**.
7. In the **Name** column, right-click **Regular Maintenance** and select **Disable**.



8. From the **File** menu, select **Exit**.

Installing Contact Center patches

Before you begin

- Download the latest documentation. See [Downloading the most recent product documentation](#) on page 220.

- Download the latest appropriate patch bundles. See [Downloading the most recent patches to the server](#) on page 221.
- Ensure that you use an account with administrator privileges on your server.
- Temporarily stop Microsoft Windows Server Automatic Maintenance while you update Contact Center software.

About this task

Install the latest Contact Center patch bundles to ensure that you have the most current development updates, or when you are upgrading your system.

The Contact Center Update Manager displays patches for installed Contact Center applications.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Update Manager**.
2. Click **Install**.
3. Click **Browse** and navigate to the folder where you downloaded the patch bundles.
4. Click **Scan for Patches**.

The Contact Center Updates section displays the available patches.

5. Select the appropriate patches.
6. Click **Install Patch(es)**.
7. On the **License Agreement** window, read the End User License Agreement and if acceptable, click **I accept the terms in the license agreement**.
8. Click **Continue**.

The Update Manager installs the patches and displays a confirmation message.

9. Click **Close**.
10. Verify that the newly installed patches appear under Installed Updates.

Next steps

Re-enable Microsoft Windows Server Automatic Maintenance.

Enabling Windows Server Automatic Maintenance

About this task

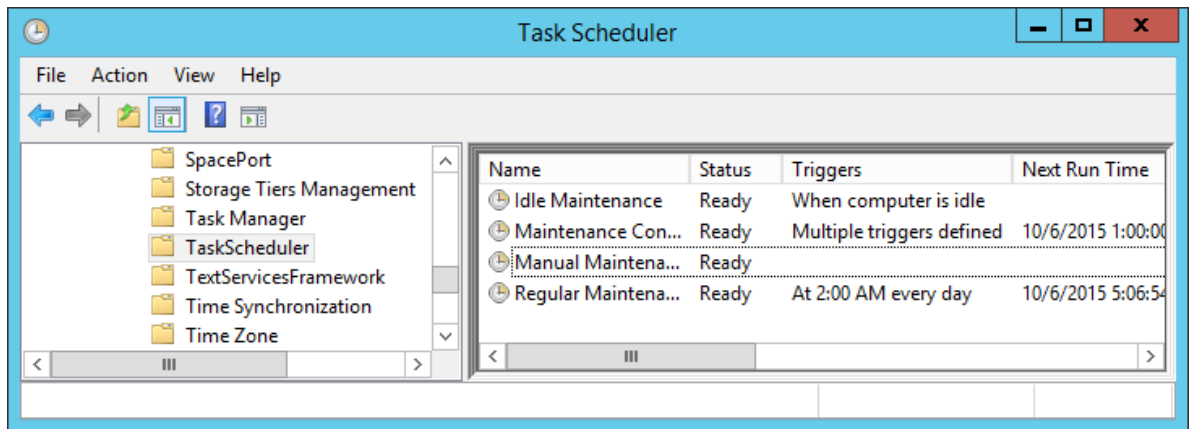
Enable Windows Server Automatic Maintenance after updating Contact Center software.

Procedure

1. Log on to the Contact Center server as Administrator.
2. On the **Desktop** screen, right-click **Start** and select **Run**.

Maintenance procedures

3. In the **Run** text box, type `Taskschd.msc`.
4. Click **OK**.
5. On the **Task Scheduler** window, in the left pane, select **Task Scheduler Library > Microsoft > Windows > TaskScheduler**.
6. In the **Name** column, right-click **Idle Maintenance** and select **Enable**.
7. In the **Name** column, right-click **Regular Maintenance** and select **Enable**.



8. From the **File** menu, select **Exit**.

Logging on to Avaya Aura[®] Media Server Element Manager

Before you begin

- Obtain a valid user name and password to access Avaya Aura[®] Media Server Element Manager.

About this task

Log on to the Avaya Aura[®] Media Server Element Manager to configure Avaya Aura[®] Media Server for Avaya Contact Center Select.

Element Manager (EM) is a web-based administration tool that facilitates the Operation, Administration, and Maintenance (OAM) of Avaya Aura[®] Media Server.

* Note:

You must have more than one Avaya Aura[®] Media Server account managed by separate users. If one account is disabled or lost, another account can perform critical tasks, backups or recovery. For more information, see *Implementing and Administering Avaya Aura[®] Media Server*.

Procedure

1. Start a Web browser.

2. In the address box, type the following URL:

```
https://SERVER_IP_ADDRESS:8443/em
```

Where SERVER_IP_ADDRESS is the IP address of the Avaya Aura® Media Server.

3. In the **User ID** box, type the Avaya Aura® Media Server User ID log on account name. The default Element Manager user account name is `Admin`.
4. In the **Password** box, type the Element Manager password. Use the `Admin` account password. The default password is `Admin123$`.
5. Click **Sign In**.

Backing up the Avaya Aura® Media Server software appliance database

About this task

Backup the Avaya Aura® Media Server software appliance database. The Avaya Aura® Media Server software appliance (OVA) does not support root access. Use this procedure to backup data on an Avaya Aura® Media Server software appliance.

Procedure

1. Log on to Avaya Aura® Media Server Element Manager.
2. Navigate to **Tools > Backup and Restore > Backup Tasks**.
3. Create or select an existing backup task that includes System Configuration and Application Content backup types.
4. Click **Run Now**.
5. To monitor the Backup and Restore History Log, navigate to **Tools > Backup and Restore > History Log**.

After the backup is complete, the log shows a completed backup task entry.

6. If you are using an FTP or SFTP backup destination, ensure that the backup files are saved to their required location.

There is one file for each backup type for a total of two backup files.

7. If you are using a local backup destination and about to perform an upgrade or redeploy of the Avaya Aura® Media Server appliance, you must move the backup files to a safe location by performing the following steps:
 - a. Log in to a Linux shell using the customer `cust` account.
 - b. Change to the public directory by using the `cdpub` alias or the following command:

```
cd /opt/avaya/app/pub
```

Maintenance procedures

- c. List the backups available on the local system by using the following command:

```
bkupFile -list
```

- d. Move the recent configuration and application data backups from the local backup storage to the current directory by using the following commands:

```
bkupFile -retrieve SystemConfiguration_backup.zip
```

```
bkupFile -retrieve ApplicationContent_backup.zip
```

- e. Save both backup files in a safe location by using the sftp file transfer tool, or another similar tool, to transfer the files off the server.
- f. After you confirm the files are safely saved, you can delete the backup files from the current directory to free disk space.

Installing Avaya Aura® Media Server patches

Before you begin

- Read the QFE Readme files for the most recent information and instructions.
- Download the most recent Avaya Aura® Media Server Quick Fix Engineering patches and store them in the QFE subdirectory on the Avaya Aura® Media Server. QFE patches are ZIP files, do not un-zip QFE patches. The Avaya Aura® Media Server patching utility uses the QFE ZIP files. The default QFE folder location is `/opt/avaya/ma/MAS/qfe`.
- Back up the Avaya Aura® Media Server data before applying patches.

About this task

Install a new Quick Fix Engineering patch to apply a change to the Avaya Aura® Media Server system. You must lock Avaya Aura® Media Server before applying patches and unlock it after you install the patches.

Note:

Follow the instructions in the Avaya Contact Center Select Release Notes and in each Avaya Aura® Media Server patch Readme file.

Procedure

1. On the Avaya Contact Center Select server, start a Web browser.
2. In the address box, type `https://<SERVER_IP_ADDRESS>:8443/em`, where `SERVER_IP_ADDRESS` is the IP address of the Avaya Aura® Media Server.
3. In the **User ID** box, type the Avaya Aura® Media Server Element Manager user name.
4. In the **Password** box, type the Avaya Aura® Media Server Element Manager password.
5. Click **Log In**.
6. In the navigation pane, click **System Status > Element Status**.

7. From the **More Actions** list, select **Pending Lock** to lock the Avaya Aura® Media Server after all processes finish.
8. Wait for existing active sessions to end.
9. In the **More Actions** menu, select **Lock**.
10. Click **Stop** and confirm the operation on the following page.
11. Close Element Manager.
12. On your Avaya Aura® Media Server, open a Linux terminal.
13. Change to the root user by running the `su -` command.
14. Obtain the correct name of the new QFE patch by entering the following command:

```
amspatch list all
```

The name of the file is not necessarily the same as the name of the patch name.
15. Under the **QFE Name** column, note the name of the patch (patchname).
16. Install all of the patches in numerical order. To install a new patch on the system, enter the following command:

```
amspatch apply <patchname>
```
17. To install all downloaded QFE patches on the system, enter the following command:

```
amspatch apply all
```
18. When the patch application is complete, open the Element Manager navigation pane, and click **Tools > Software Inventory**.
19. Verify the patch version listed in the **Patch Level** column is correct.
20. Select **System Status > Element Status**, and click **Start**. Confirm the operation.
21. From the **More Actions** list, select **Unlock** to unlock the Avaya Aura® Media Server.
22. Select **System Status > Alarms** and check for service-impacting alarms.

Starting or stopping Contact Center server services

Before you begin

- Ensure there are no active calls before stopping the Avaya Contact Center Select services.

About this task

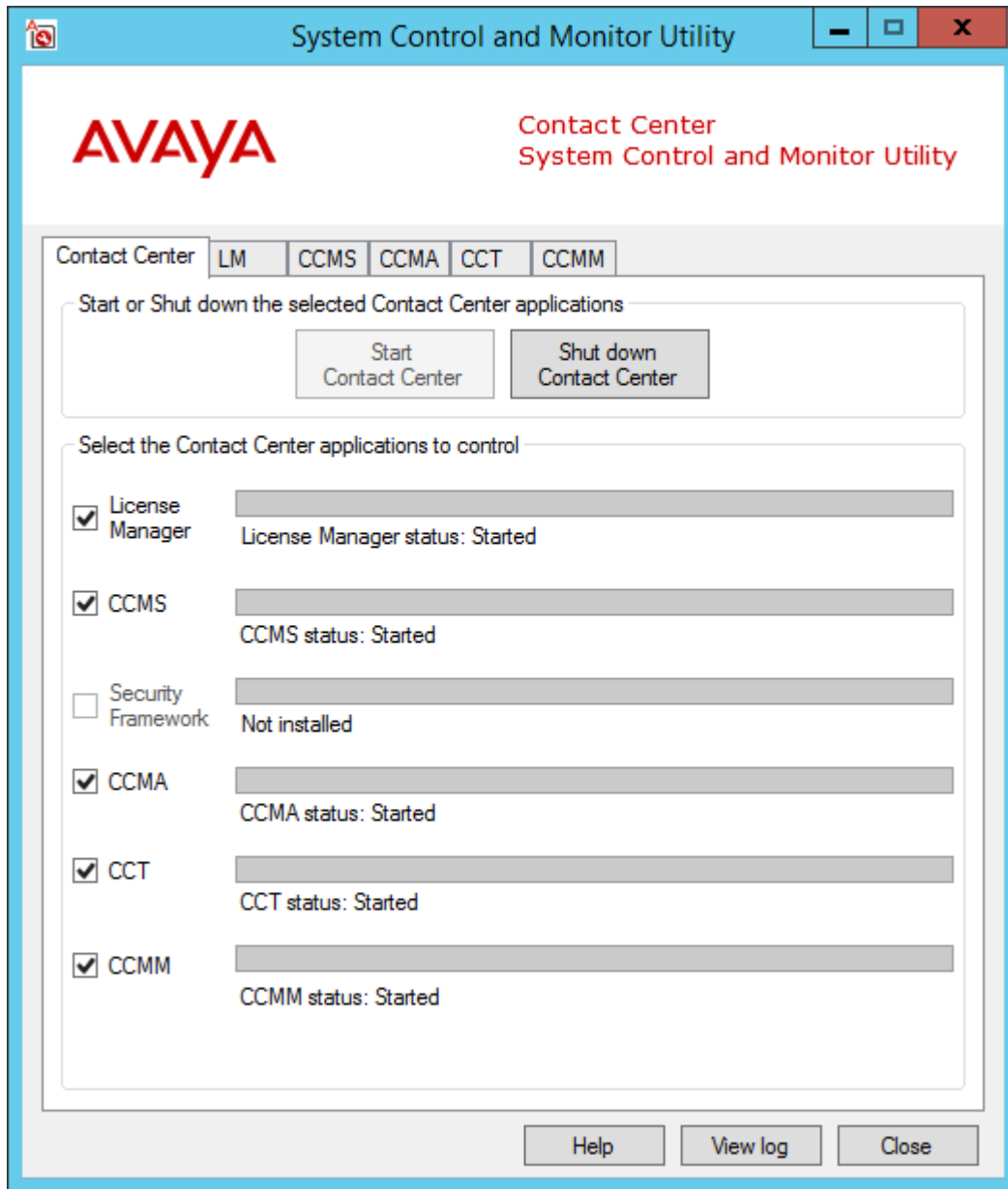
Use the System Control and Monitor Utility to start or stop all Avaya Contact Center Select services.

Procedure

1. Log on to the Avaya Contact Center Select server.

Maintenance procedures

2. On the **Apps** screen, in the **Avaya** section, select **System Control and Monitor Utility**.
3. Click the **Contact Center** tab.



4. To start the Avaya Contact Center Select services, click **Start Contact Center**.
5. To stop the Avaya Contact Center Select services, click **Shut down Contact Center**.

Rebooting the Avaya Aura® Media Server virtual machine

About this task

Reboot the Avaya Aura® Media Server virtual machine. Some maintenance tasks and configuration procedures require you to reboot the server.

Procedure

1. Using an SSH client, access the Avaya Aura® Media Server Linux shell console using the `cust` account details.
2. On the command line, enter `reboot`.
3. Enter `y` to continue with the reboot.

The Avaya Aura® Media Server virtual machine reboots.

Shutting down the Avaya Aura® Media Server virtual machine

About this task

Shut down the Avaya Aura® Media Server virtual machine. Some maintenance tasks and configuration procedures require you to shutdown the server.

Procedure

1. Using an SSH client, access the Avaya Aura® Media Server Linux shell console using the `cust` account details.
2. On the command line, enter `shutdown`.
3. Enter `y` to continue with the shutdown.

The Avaya Aura® Media Server virtual machine shuts down.

Part 7: Customization

Chapter 17: Customizing the solution

This section describes how to customize the working contact center for your solution. The default configuration is an example of a generic contact center solution. You can now customize Avaya Contact Center Select to meet your requirements.

Avaya Contact Center Select provides sample data to minimize the time and effort needed to validate basic contact center operation. You can also use the sample data provided as the initial configuration for your solution. When you log on to Contact Center Manager Administration for the first time, the following sample data is visible in the Management and Configuration components:

- Two sample supervisors, each created as a Supervisor/Agent. Contact Center creates a local Windows user account on the server linked to each of these supervisor agents.
- Eight sample agents, each assigned to one of the two sample supervisor/agents. Contact Center creates a local Windows user account on the server linked to each of these agents
- Two sample voice skillsets.
- One sample Agent Skillset Assignment and one sample Agent Supervisor Assignment.
- A sample skillset for each of the supported contact types. Each sample agent is assigned to the voice skillset.
- Sample Activity codes, After Call Work Item codes, and Not Ready Reason codes.
- A sample CDN (Route Point) number for voice calls.
- A sample Open Queue Route Point for multimedia contacts.
- Two sample Multiplicity Presentation Classes. A Multiplicity Presentation Class enables an agent to handle more than one contact type concurrently.
- One sample Route to provide music on a customer call.
- Three sample Threshold Classes with preconfigured values. Threshold classes determine how statistics are presented on real-time and historical reports.

Avaya Contact Center Select Prompt Management allows the administrator to manage prompts on the Avaya Aura[®] Media Server (Avaya Aura[®] MS). Contact Center provides a number of sample prompts and sample music that you can use in your Orchestration Designer flow applications to treat Contact Center calls. Contact Center also provides sample Orchestration Designer flow applications that use the sample prompts and music provided, in addition to the standard Orchestration Designer flows available previously. All of the sample prompts have an associated variable that exists in Orchestration Designer. This allows the administrator to modify the prompts within the flow applications without opening Orchestration Designer.

Contact Center uses the sample CDN (Route Point) number to deliver calls to the sample Customer_Service flow application. The Customer_Service flow application provides sample treatments and routes the call to a sample agent.

The sample data provided allows you to make a first routed call in your contact center. It also serves as your initial configuration and allows you to rapidly commission your Avaya Contact Center Select solution.

Default user accounts

Account name	Password	Description
Administrator	Administrator	Default Contact Center Manager Administration administrator user.
reporting1	reporting1	A default Contact Center Manager Administration supervisor user.
reporting2	reporting2	A default Contact Center Manager Administration supervisor user.

Configuring Internet Explorer

About this task

Configure Internet Explorer to access Contact Center Manager Administration.

Install Microsoft Internet Explorer 10.0 or 11.0 (32 bit or 64 bit versions). Contact Center Manager Administration supports both the 32 bit and 64 bit versions of Microsoft Internet Explorer.

 **Note:**

You must run Internet Explorer in compatibility mode for Contact Center Manager Administration.

Procedure

1. Start Internet Explorer.
2. From the menu, select **Tools > Internet Options**.
3. In the **Internet Options** dialog box, click the **Security** tab.
4. Click the **Trusted Sites** icon.
5. Click **Custom Level**.
6. In the **Security Settings** dialog box for trusted sites, under the **.NET Framework-reliant components** heading, select **Enable** for the following:
 - **Run components not signed with Authenticode**
 - **Run components signed with Authenticode**
7. Under the **ActiveX controls and plug-ins** heading, select **Enable** for the following:
 - **Download signed ActiveX controls**
 - **Run ActiveX Controls and plug-ins**

- **Script ActiveX Controls marked safe for scripting**
8. Under the **Downloads** heading, select **Enable** for the following:
 - **Automatic prompting for file downloads**
 - **File download**
 9. Under the **Miscellaneous** heading, for **Allow script-initiated windows without size or position constraints**, select **Enable**.
 10. Under the **Miscellaneous** heading, for **Allow websites to open windows without address or status bars**, select **Enable**.
 11. Under **Reset custom settings**, from the **Reset to:** list select **Medium-low**.
 12. Click **Reset**.
 13. On the Warning dialog box, click **Yes**.
 14. Click **OK**.
 15. If you enabled ActiveX options, when a message appears asking you to confirm your choice, click **Yes**.
 16. Click the **Trusted Sites** icon.
 17. Click **Sites**.
 18. In the **Trusted sites** dialog box, clear the **Require server verification {https:} for all sites in this zone** check box.
 19. In the **Add this Web site to the zone** box, type the server name (not the IP address) for your Avaya Contact Center Select server.
 20. Click **Add**.
 21. Click **Close** to return to the **Internet Options** dialog box.
 22. Click the **Privacy** tab.
 23. In the **Pop-up Blocker** section, select the **Block pop-ups** check box.
 24. Click **Settings**.
 25. In the **Pop-up Blocker Settings** dialog box, in the **Address of website to allow** box, type the Avaya Contact Center Select server URL, `http://<server name>/`, where `<server name>` is the name of the Avaya Contact Center Select server.
 26. Click **Add**.
 27. Click **Close**.
 28. In the **Internet Options** dialog box, click the **Advanced** tab.
 29. Under **Browsing**, clear the **Reuse windows for launching shortcuts** check box.
 30. Click **OK** to exit the **Internet Options** dialog box.
 31. Restart Internet Explorer to activate your changes.

Accessing CCMA using Microsoft Edge with Internet Explorer mode

You can access CCMA in the Microsoft Edge browser using Internet Explorer (IE) mode. To enable IE mode in Microsoft Edge, you must perform the following procedures:

1. [Adding the Microsoft Edge administrative templates](#) on page 234.
2. [Configuring Internet Explorer integration](#) on page 235.
3. [Configuring the Enterprise Mode Site List](#) on page 236.

Before enabling IE mode in Microsoft Edge, ensure that you install all recent Windows updates and use Microsoft Edge version 77 or later.

Ensure that you install Microsoft Edge at the system level. You can check it by typing `edge://version` in the Microsoft Edge address bar. The executable path must start with `C:\Program Files`, which indicates a system install.

For more information about IE mode in Microsoft Edge, refer to the Microsoft documentation.

Important:

- You must not delete the Internet Explorer 11 browser from your computer, otherwise Microsoft Edge cannot launch CCMA.
- Always launch CCMA in a new tab of Microsoft Edge.
- If you enable single sign-on (SSO) on your Contact Center, you must add the System Manager (SMGR) server FQDN to the Enterprise Mode Site List.
- For solutions with geographic redundancy, you must add the RGN server short name and FQDN to the Enterprise Mode Site List.
- For Business Continuity solutions, you must add only the Managed Name and Managed FQDN of the BC pair to the Enterprise Mode Site List. Do not add short names and FQDNs of your active and standby servers.

Adding the Microsoft Edge administrative templates

About this task

Use this procedure to add the Microsoft Edge administrative templates to your computer.

Before you begin

Download and install Microsoft Edge version 77 or later.

Procedure

1. On the Microsoft website, go to the **Edge for Business** download page: <https://www.microsoft.com/en-us/edge/business/download>.
2. From the lists, select your current browser version, build, and platform.
3. Click the **GET POLICY FILES** button.

4. Click **Accept and download** to download the `MicrosoftEdgePolicyTemplates` file.
The `MicrosoftEdgePolicyTemplates` archive is downloaded to the default folder on your computer.
5. Unzip the `MicrosoftEdgePolicyTemplates` archive.
6. Open the `MicrosoftEdgePolicyTemplates` folder and navigate to `windows\admx`.
7. From the `admx` folder, copy the `msedge.admx` file.
8. Navigate to `C:\Windows\PolicyDefinitions` and paste the `msedge.admx` file to the `PolicyDefinitions` folder.
9. In the `admx` folder, open the required language folder.
For example, for the United States, open the `en-US` folder.
10. From the language folder, copy the `msedge.adml` file.
11. Navigate to `C:\Windows\PolicyDefinitions` and paste the `msedge.adml` file to the matching language folder in the `PolicyDefinitions` folder.
12. **(Optional)** Verify that you have added the Microsoft Edge administrative template correctly by doing the following:
 - a. Press `Win+R` and run `gpedit.msc` to open the Local Group Policy Editor.
 - b. Click **Computer Configuration > Administrative Templates**.

The `Administrative Templates` folder contains folders with the Microsoft Edge administrative templates.

Next steps

Configure Internet Explorer integration using Local Group Policy Editor.

Configuring Internet Explorer integration

About this task

Use this procedure to configure Internet Explorer integration using Local Group Policy Editor.

Before you begin

Add the Microsoft Edge administrative templates to your computer.

Procedure

1. Press `Win+R` and run `gpedit.msc` to open the Local Group Policy Editor.
2. Click **Computer Configuration > Administrative Templates > Microsoft Edge**.
Local Group Policy Editor displays the Microsoft Edge pane.
3. In the Microsoft Edge pane, double-click **Configure Internet Explorer integration**.
The system displays the Configure Internet Explorer integration window.

4. In the Configure Internet Explorer integration window, select **Enabled**.
5. From the **Configure Internet Explorer integration** list, select **Internet Explorer mode**.
This is a default option for accessing CCMA in Microsoft Edge.
6. Click **OK**.

Result

IE mode in Microsoft Edge is now enabled.

Next steps

Configure the site list that you want to access using IE mode in Microsoft Edge.

Configuring the Enterprise Mode Site List

About this task

Use this procedure to configure the Enterprise Mode Site List.

On your computer, create an XML file with the list of sites that you want to access using Microsoft Edge with IE mode.

The XML file must contain the following elements:

- **site-list version** number: Internet Explorer uses this number to verify whether the site list is new. Approximately 65 seconds after Internet Explorer 11 starts, it compares your site list version to the stored version number. You must increase the site-list version number every time you update the version of the Enterprise Mode Site List.
- **<compat-mode>** tag: This tag specifies the compatibility settings for a specific site or domain. Use the `default` value.
- **<open-in>** tag: This tag specifies which Internet Explorer version opens for a specific site or domain. Use the `IE11` version.

Before you begin

- Add the Microsoft Edge Policy templates to your computer.
- Configure Internet Explorer integration.
- Ensure that you have your Contact Center server short name and FQDN.
- If you enable SSO on your Contact Center, ensure that you have your SMGR server FQDN.
- For a solution with geographic redundancy, ensure that you know your RGN server short name and FQDN.
- For a BC solution, ensure that you have your BC pair Managed Name and Managed FQDN.

Procedure

1. On your computer, create the `sites.xml` file using the following template:

```
<site-list version="1">
  <!-- File creation header -->
  <created-by>
    <tool>EnterpriseSitelistManager</tool>
```

```

        <version>10240</version>
        <date-created>20200717.142200</date-created>
    </created-by>
    <!-- Begin Site List -->
    <site url="server short name">
        <compat-mode>default</compat-mode>
        <open-in>IE11</open-in>
    </site>
    <site url="server FQDN">
        <compat-mode>default</compat-mode>
        <open-in>IE11</open-in>
    </site>
</site-list>

```

2. In the first `<site>` element, for the `url` attribute, type the Contact Center server short name.

For example, if your Contact Center server short name is `auracc12680`, the code must look as follows: `<site url="auracc12680">`.

For a BC solution, you must use your BC pair Managed Name instead of the server short name.

3. In the second `<site>` element, for the `url` attribute. type the Contact Center server FQDN.

For example, if your Contact Center server FQDN is `auracc12680.aacc7dc2012.com`, the code must look as follows: `<site url="auracc12680.aacc7dc2012.com">`.

For a BC solution, you must use your BC pair Managed FQDN instead of the server FQDN.

4. **(Optional)** Add your SMGR server to the site list using the following template:

```

<site url="SMGR server FQDN">
    <compat-mode>default</compat-mode>
    <open-in>IE11</open-in>
</site>

```

For example, if your SMGR server FQDN is `smgr80176.aacc7dc2012.com`, the code must look as follows: `<site url="smgr80176.aacc7dc2012.com">`.

5. **(Optional)** Add your RGN server to the site list using the following template:

```

<site url="RGN server short name">
    <compat-mode>default</compat-mode>
    <open-in>IE11</open-in>
</site>
<site url="RGN server FQDN">
    <compat-mode>default</compat-mode>
    <open-in>IE11</open-in>
</site>

```

6. Press `Win+R` and run `gpedit.msc` to open the Local Group Policy Editor.
7. Click **Computer Configuration > Administrative Templates > Microsoft Edge**.
Local Group Policy Editor displays the Microsoft Edge pane.
8. In the Microsoft Edge pane, double-click **Configure the Enterprise Mode Site List**.

Local Group Policy Editor displays the Configure the Enterprise Mode Site List window.

9. In the Configure the Enterprise Mode Site List window, select **Enabled**.
10. In the Options field, type the `sites.xml` location.
For example: `file:///c:/Users/user_name/Documents/sites.xml`.
11. Click **OK**.
12. **(Optional)** In the Microsoft Edge address bar, type `edge://compat/enterprise` and press `Enter`.

Microsoft Edge displays the Enterprise Mode Site List page, where you can view the current list of sites that Microsoft Edge opens in IE mode. Microsoft Edge automatically checks if there is a newer site list version and updates it approximately 65 seconds after launch, however, you can also manually configure Microsoft Edge to use the latest site list version by clicking the **Force update** button.

Next steps

Launch Microsoft Edge and wait for approximately 65 seconds. You can now access CCMA using Microsoft Edge with IE mode.

Internet Explorer mode and Compatibility View configuration on the domain server

If you cannot configure Internet Explorer (IE) mode or Compatibility View from a local computer, you can configure these settings on the domain server. For example, if you cannot use Internet Explorer according to your enterprise security policies, you can only configure Compatibility View settings on the domain server.

To enable IE mode for Microsoft Edge on the domain server, perform the following procedures:

1. [Adding the Microsoft Edge administrative templates to the domain server](#) on page 239.
2. [Creating a configuration file for IE mode](#) on page 240.
3. [Enabling IE mode on the domain server](#) on page 243.
4. [Completing IE mode configuration on a local computer](#) on page 244.

To enable Compatibility View on the domain server, perform procedure [Configuring Compatibility View settings on the domain server](#) on page 245.

If required, you can disable Internet Explorer from the domain server as described in [Disabling Internet Explorer 11 as a standalone browser](#) on page 246.

For more information about IE mode in Microsoft Edge and Compatibility View, refer to the Microsoft documentation.

! Important:

- You must not delete the Internet Explorer 11 browser from your computer, otherwise Microsoft Edge cannot launch CCMA.
- Always launch CCMA in a new tab of Microsoft Edge.
- If you enable single sign-on (SSO) on your Contact Center, you must also add the System Manager (SMGR) server FQDN to the Enterprise Mode Site List.
- For solutions with geographic redundancy, you must add the RGN server short name and FQDN to the Enterprise Mode Site List.
- For Business Continuity solutions, you must add only the Managed Name and Managed FQDN of the BC pair to the Enterprise Mode Site List. Do not add short names and FQDNs of your active and standby servers.
- If you use Windows 11, ensure that you use Contact Center Release 7.1.2 and the latest post GA path bundle.

Adding the Microsoft Edge administrative templates to the domain server

About this task

Use this procedure to add the Microsoft Edge administrative templates to the domain server.

Procedure

1. On the Microsoft website, go to the **Edge for Business** download page: <https://www.microsoft.com/en-us/edge/business/download>.
2. Click the **GET POLICY FILES** button.
3. Click **Accept and download** to download the `MicrosoftEdgePolicyTemplates` file.
The `MicrosoftEdgePolicyTemplates` archive is downloaded to the default folder on your computer.
4. Unzip the `MicrosoftEdgePolicyTemplates` archive.
5. Open the `MicrosoftEdgePolicyTemplates` folder and navigate to `windows\admx`.
6. From the `admx` folder, copy the `msedge.admx` file.
7. Upload the `msedge.admx` file to the domain server to the `C:\Windows\PolicyDefinitions` folder.
Use a file transfer program of your choice, such as SFTP, SCP, or WinSCP.
8. On your local computer, re-open the `MicrosoftEdgePolicyTemplates` folder and navigate to the `windows\admx\` folder.
9. In the `admx` folder, open a folder corresponding to the language and locale you use on Contact Center.

For example, for the United States, open the `en-US` folder.

10. From the language folder, copy the `msedge.adml` file.
11. Upload the `msedge.adml` file to the domain server to the `C:\Windows\PolicyDefinitions\<LANGUAGE_FOLDER>` folder.

In this file path, `<LANGUAGE_FOLDER>` is the language folder with the same name that you selected in step 9. For example, for the United States, copy `msedge.adml` to the `C:\Windows\PolicyDefinitions\en-US` folder.

Next steps

Create a configuration file for IE mode.

Creating a configuration file for IE mode

About this task

You must create an XML file that contains a list of sites you need to access from Microsoft Edge using IE mode. You will use this file to configure the Enterprise Mode Site List on the domain server.

The XML file must contain the following elements:

- **site-list version** number: Internet Explorer uses this number to verify whether the site list is new. Approximately 65 seconds after Internet Explorer 11 starts, it compares your site list version to the stored version number. You must increase the site-list version number every time you update the version of the Enterprise Mode Site List.
- **<compat-mode>** tag: This tag specifies the compatibility settings for a specific site or domain. Use the `default` value.
- **<open-in>** tag: This tag specifies which Internet Explorer version opens for a specific site or domain. Use the `IE11` version.

Before you begin

- Add the Microsoft Edge Policy templates to the domain server.
- Ensure that you have your Contact Center server short name and FQDN.
- If you enable SSO on your Contact Center, ensure that you have your SMGR server FQDN.
- For a solution with geographic redundancy, ensure that you know your RGN server short name and FQDN.
- For a BC solution, ensure that you have your BC pair Managed Name and Managed FQDN.

Procedure

1. Create an XML file using the following template:

```
<site-list version="1">
  <!-- File creation header -->
  <created-by>
    <tool>EnterpriseSitelistManager</tool>
    <version>10240</version>
    <date-created>20200717.142200</date-created>
```



```

</created-by>
<!-- Begin Site List -->
<site url="<SERVER SHORT NAME>">
  <compat-mode>default</compat-mode>
  <open-in>IE11</open-in>
</site>
<site url="<SERVER FQDN>">
  <compat-mode>default</compat-mode>
  <open-in>IE11</open-in>
</site>
</site-list>

```

2. In the first `<site>` element, for the `url` attribute, type the short name of your Contact Center server.

For example, if the short name of your Contact Center server is `auracc12680`, the code must look as follows:

```
<site url="auracc12680">
```

For a BC solution, you must use your BC pair Managed Name instead of the server short name.

3. In the second `<site>` element, for the `url` attribute, type the Contact Center server FQDN.

For example, if your Contact Center server FQDN is `auracc12680.aacc7dc2012.com`, the code must look as follows:

```
<site url="auracc12680.aacc7dc2012.com">
```

For a BC solution, you must use your BC pair Managed FQDN instead of the server FQDN.

4. **(Optional)** If you use SSO on your Contact Center, add a new `<site>` element for your System Manager to the file using the following template:

```

<site url="SMGR server FQDN">
  <compat-mode>default</compat-mode>
  <open-in>IE11</open-in>
</site>

```

For example, if your System Manager FQDN is `smgr80176.aacc7dc2012.com`, the code must look as follows:

```

<site url="smgr80176.aacc7dc2012.com">
  <compat-mode>default</compat-mode>
  <open-in>IE11</open-in>
</site>

```

5. **(Optional)** For a solution with geographic redundancy, add a new `<site>` element for your RGN server to the site list using the following template:

```

<site url="RGN server short name">
  <compat-mode>default</compat-mode>
  <open-in>IE11</open-in>
</site>
<site url="RGN server FQDN">
  <compat-mode>default</compat-mode>
  <open-in>IE11</open-in>
</site>

```

6. Save the file using the `sites.xml` name.

Next steps

- Upload the configuration file to one of the following locations:
 - To the CCMA server. For more information about uploading the file to the CCMA server, see [Uploading the configuration file for IE mode to the CCMA server](#) on page 242.
 - To a shared folder on the domain server.
- Enable IE mode on the domain server.

Uploading the configuration file for IE mode to the CCMA server

About this task

You can store the configuration file `sites.xml` for IE mode on the CCMA server.

Before you begin

Create the configuration file `sites.xml` for IE mode.

Procedure

1. Copy the `sites.xml` file to the CCMA server to the `D:\Avaya\Contact Center\Manager Administration\Apps` folder.

Use a file transfer program of your choice, such as SFTP, SCP, or WinSCP.

2. If you use SSO, do the following:
 - a. Add the following entry to the `AgentPromValues.xml` file, which is located in the `D:\Avaya\Contact Center\Manager Administration\Server\Data` folder:

```
<NOT_ENFORCED value="sites.xml*" />
```
 - b. On the Contact Center, disable SSO.
 - c. Re-enable SSO.

3. In Microsoft Edge or Internet Explorer, type the following URL:

```
https://<CCMA_FQDN>/sites.xml
```

In this URL, `<CCMA_FQDN>` is the FQDN of the CCMA server.

4. Ensure that you can view the `sites.xml` file contents in the browser.

Next steps

Enable IE mode on the domain server.

Enabling IE mode on the domain server

About this task

Enable IE mode on the domain server to access CCMA from Microsoft Edge.

Before you begin

- Add the Microsoft Edge Policy templates to your computer.
- Create the configuration file `sites.xml` for IE mode.
- Upload the configuration file to one of the following locations:
 - To the CCMA server. For more information about uploading the file to the CCMA server, see [Uploading the configuration file for IE mode to the CCMA server](#) on page 242.
 - To a shared folder on the domain server.

Procedure

1. On the domain server, navigate to **Control Panel > Administrative tools > Group Policy Management**.
2. Go to your domain.
3. Right-click the domain group policy and click **Edit**.
4. In the Group Policy Management Editor, go to **Computer Configuration > Policies > Administrative Templates > Microsoft Edge**.
The Group Policy Management Editor displays the Microsoft Edge pane.
5. In the Microsoft Edge pane, double-click **Configure Internet Explorer integration**.
6. In the Configure Internet Explorer Integration window, select **Enabled**.
7. In the Options area, from **Configure Internet Explorer integration**, select one of the following:
 - **Internet Explorer mode**: To open sites in Microsoft Edge in IE mode.
 - **Internet Explorer 11**: To open sites in a standalone Internet Explorer window.
 - **None**: To prevent users from configuring IE mode using `edge://flags` or CLI.
8. Click **OK**.
9. In the Group Policy Management Editor, go to **Computer Configuration > Policies > Administrative Templates > Microsoft Edge**.
10. In the Microsoft Edge pane, double-click **Configure the Enterprise Mode Site List**.
11. In the Configure the Enterprise Mode Site List window, select **Enabled**.
12. In the Options area, from **Configure the Enterprise Mode Site List**, specify the location of the `sites.xml` configuration file as follows:
 - If the `sites.xml` file is on the CCMA server, use the following format:
`https://<CCMA FQDN>/sites.xml`

In this entry, <CCMA_FQDN> is the FQDN of the CCMA server. For example:

```
https://192.0.2.1/sites.xml
```

- If the `sites.xml` file is in a shared folder on the domain server, use the following format:

```
\\<NETWORK_PATH>\sites.xml
```

In this entry, <NETWORK_PATH> is the full path to the `sites.xml` on the domain server. For example:

```
\\198.51.100.1\Shared\sites.xml
```

13. Click **OK** to save the policy settings.

Next steps

Complete IE mode configuration on a client computer.

Completing IE mode configuration on a local computer

About this task

After configuring IE mode on the domain server, update group policies on the local computer you use to access CCMA and ensure you can access CCMA using Microsoft Edge.

Before you begin

- Configure IE mode on the domain server.
- Ensure that the operating system and Microsoft Edge browser installed on your local computer comply with the system requirements for IE mode listed at <https://docs.microsoft.com/en-us/deployedge/edge-ie-mode>.

Procedure

1. On your local computer, run the following command:

```
gpupdate /force
```

2. To check if Group Policy Objects are applied, run the following command:

```
gpresult /r
```

In the command output, the Applied Group Policy Objects section must contain the domain group policy name that you configured on the domain server.

3. In the Microsoft Edge address bar, type `edge://compat/enterprise` and ensure that the Enterprise Mode Site List tab contains the `sites.xml` file you added to the domain server.
4. In Microsoft Edge, open the CCMA site.

Next steps

Configure the Compatibility View List on the domain server.

Configuring Compatibility View settings on the domain server

About this task

Compatibility View is a feature that enables Internet Explorer to open websites that are incompatible with the latest Internet Explorer versions. If Microsoft Edge cannot display the CCMA site even in IE mode, you can configure Compatibility View settings for the CCMA site. If you cannot configure the Compatibility View settings on your local computer, you can configure them on the domain server.

Windows 11 does not support Internet Explorer. Therefore, if you use Windows 11, you do not need to enable Compatibility View.

Important:

If you change Compatibility View settings, you must delete a registry key that you add to Group Policy Objects in this procedure and add it again.

Procedure

1. On the domain server, start the Internet Explorer.
2. Click the **Tools** icon and then click **Compatibility View Settings**.
Internet Explorer displays the Compatibility View Settings window.
3. In **Add this website**, type your domain name and then click **Add**.
4. On the domain server, go to **Control Panel > Administrative tools > Group Policy Management**.
5. Select your domain.
6. Right-click the domain group policy and click **Edit**.
You can also create a new domain group policy and link it to the domain.
7. In the Group Policy Management Editor, go to **User Configuration > Preferences > Windows Settings > Registry**.
8. Right-click **Registry** and click **New > Registry Wizard**.
9. In the Registry Wizard, select the local machine and then navigate to **HKEY_CURRENT_USER > Software > Microsoft > Internet Explorer > BrowserEmulation > ClearableListData**.
10. Select the check box for the **UserFilter** parameter.
11. Click **Finish**.
12. On your local computer, to update the group policy settings, run the following command:

```
gpupdate /force
```
13. To check if Group Policy Objects are applied, run the following command:

```
gpresult /r
```

In the command output, the Applied Group Policy Objects section must contain the domain group policy name that you configured on the domain server.

14. **(Optional)** Verify that the registry key `HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\BrowserEmulation\ClearableListData\UserFilter` contains the same value that is configured on the domain server.
15. Restart Internet Explorer to apply changes in the Compatibility View settings.

Disabling Internet Explorer 11 as a standalone browser

About this task

Disable Internet Explorer 11 as a standalone browser to force users in your domain to use Microsoft Edge. When users try to open shortcuts or files associated with Internet Explorer 11, they open URLs in Microsoft Edge instead.

Before you begin

Ensure that the operating system and Microsoft Edge browser installed on your local computer comply with the system requirements for IE mode listed at <https://docs.microsoft.com/en-us/deployedge/edge-ie-disable-ie11>.

Procedure

1. On the domain server, navigate to **Control Panel > Administrative Tools > Group Policy Management**.
2. Go to your domain.
3. Right-click the domain policy and click **Edit**.
You can also create a new domain policy and link it to the domain.
4. In the Group Policy Management Editor, go to **Computer Configuration > Policies > Administrative Templates > Windows components > Internet Explorer**.
5. In the Microsoft Edge pane, double-click **Disable Internet Explorer 11 as a standalone browser** and select **Enabled**.
6. In the Options area, select one of the following:
 - **Never**: To notify the users that Internet Explorer 11 is disabled.
 - **Always**: To notify the users every time they are redirected from Internet Explorer 11.
 - **Once per user**: To notify the users only the first time they are redirected.
7. Click **OK**.
8. Log in to a computer in the domain and run the `gpupdate /force` command.
9. **(Optional)** To check if Group Policy Objects are applied, run the `gpresult /r` command.
10. Open Internet Explorer.

You can see the following message: This action is restricted. For more information, please contact your system administrator.

Starting the Script Variables tool in Contact Center Manager Administration

Before you begin

- Ensure the client computer meets the administration client computer requirements. For more information, see *Avaya Contact Center Select Solution Description*.
- Configure Internet Explorer. For more information, see [Configuring Internet Explorer](#) on page 232.

About this task

Start the Script Variables tool to list the application variables on your system. You can also use this window to create, update, or delete an application variable.

You can log on to CCMA for the first time as an administrator or a supervisor. For security reasons, Avaya recommends that you change the default password when you first log on to the application. CCMA user passwords can contain only English characters and special characters.

Procedure

1. Start Internet Explorer.
2. In the **Address** box, type the URL of the Avaya Contact Center Select server. The default URL is `http://<server name>`, where `<server name>` is the host name of the Avaya Contact Center Select server.
3. Press **Enter**.
4. In the main logon window, in the **User ID** box, type the user name. The default user ID is Administrator.
5. In the **Password** box, type the password. The default user password is Administrator.
6. Click **Log In**.
7. From the **Launchpad**, select **Scripting**.
8. In the Scripting window, expand the system tree.
9. In the left pane, in the system tree, click your Contact Center Manager Server.
10. Click **Script Variables**.

Checking variables for referencing applications

Before you begin

- Start the Script Variables tool. See [Starting the Script Variables tool in CCMA](#) on page 247.

About this task

Check a variable to see if it is referenced by an active application. If it is referenced by an active application, you can change the value of the variable or the comment.

If you want to change the properties of a variable and how the variable appears in an application, you can deactivate the application or remove the reference to the variable from the referencing application.

Procedure

1. In the Scripting window, expand the system tree.
2. In the system tree, click **CC**.
3. Click **Script Variables**.

The system tree in the left pane expands to show all types of variables. The right pane shows an alphabetical list of all variables. In the Script Variables grid, you can sort all columns by clicking on the column header.

4. In the left pane of the Script Variables window, select the script variable that you want to check.
5. In the right pane, click **Script Variable Properties**.
6. Under **Referencing Scripts**, determine which scripts use the variable.
7. View the **Script Variable Properties** to change the variable value or comment.
8. Click **Submit**.

Configuring business and public holiday dates

Before you begin

- Start the Contact Center Manager Administration Script Variables tool. See [Starting the Script Variables tool in CCMA](#) on page 247.
- Ensure that the variable is not referenced by an active application. See [Checking variables for referencing applications](#) on page 248.

About this task

Configure the dates on which the contact center is closed. For example, add the local business and public holidays to the list of contact center holidays.

Avaya recommends that you add your local business and public holidays and remove the sample dates.

Procedure

1. From the Contact Center Manager Administration **Launchpad**, select **Scripting**.
2. In the Scripting window, expand the system tree.
3. In the system tree, click your Avaya Contact Center Select server.
4. Click **Script Variables**.

The system tree in the left pane expands to show all types of variables. The right pane shows an alphabetical list of all variables. In the Script Variables grid, you can sort all columns by clicking on the column header.

5. In the Script Variables window, select the script variable that you want to change. Expand **Date** and select **holidays_gv**.
6. Click **Script Variable Properties**.
7. In the **Script Variable Properties** property sheet, select the **Attribute** tab.

The screenshot shows the Avaya Scripting interface. The left pane displays a system tree with 'Script Variables' expanded. The main pane shows a table of 'Script Variables [Full Control]' for server 'CC'. The table lists 'contact_cbdate_cv' and 'holidays_gv'. Below the table, the 'Script Variable Properties' dialog is open for 'holidays_gv', showing the 'Attribute' tab. The dialog includes a 'Name' field with 'holidays_gv', radio buttons for 'Global Variable' (selected) and 'Call Variable', a 'Comment' field with the text 'This global variable contains sample holiday e.g. Jan 1st', and a 'Referencing Scripts' table listing 'Customer_Service'.

Name	Scope	Type	Used in Script	Modified By	Last Modified
contact_cbdate_cv	Call	DATE	No	Web, Administrator	7/3/2009 4:18:47 PM
holidays_gv	Global	DATE	Yes	Web, Administrator	6/30/2015 8:55:19 AM

Name
Customer_Service
*

8. In the **List of Values** table, add your local business and public holidays.
9. If any of the existing dates are not suitable for your solution, use the **Remove** button to delete the dates.
10. Click any other row in the table to save the dates.

11. Click **Submit**.

Configuring the office hours

Before you begin

- Start the Contact Center Manager Administration Script Variables tool. See [Starting the Script Variables tool in CCMA](#) on page 247.
- Ensure that the variable is not referenced by an active application. See [Checking variables for referencing applications](#) on page 248.

About this task

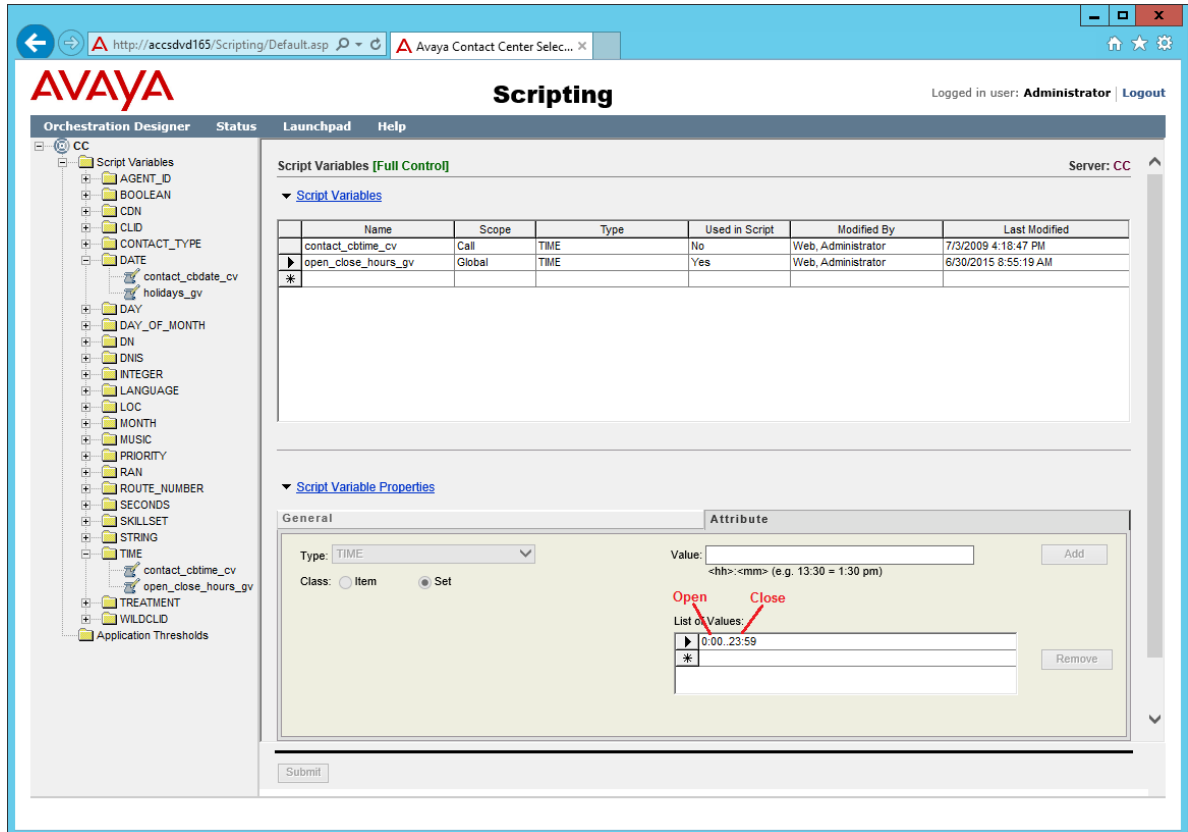
Configure the time of day that your solution is open for business.

Procedure

1. From the Contact Center Manager Administration **Launchpad**, select **Scripting**.
2. In the Scripting window, expand the system tree.
3. In the system tree, click your Avaya Contact Center Select server.
4. Click **Script Variables**.

The system tree in the left pane expands to show all types of variables. The right pane shows an alphabetical list of all variables. In the Script Variables grid, you can sort all columns by clicking on the column header.

5. In the Script Variables window, select the script variable that you want to change. Expand **TIME** and select **open_close_hours_gv**.
6. Click **Script Variable Properties**.
7. In the **Script Variable Properties** property sheet, select the **Attribute** tab.



8. In the **List of Values** table, edit the time of day that your contact center opens. This is the first time in the list. The default is 00:00.
9. In the **List of Values** table, edit the time of day your contact center closes. This is the second time in the list. The default is 23:59.
10. Click **Submit**.

Changing the default voice mail number

Before you begin

- Start the Contact Center Manager Administration Script Variables tool. See [Starting the Script Variables tool in CCMA](#) on page 247.
- Ensure that the variable is not referenced by an active application. See [Checking variables for referencing applications](#) on page 248.

About this task

Change the default voice mail number to match your solution. This voice mail number is used by "Option 4" in the Customer Service sample Orchestration Designer flow application.

Procedure

1. From the Contact Center Manager Administration **Launchpad**, select **Scripting**.
2. In the Scripting window, expand the system tree.
3. In the system tree, click your Avaya Contact Center Select server.
4. Click **Script Variables**.

The system tree in the left pane expands to show all types of variables. The right pane shows an alphabetical list of all variables. In the Script Variables grid, you can sort all columns by clicking on the column header.

5. In the Script Variables window, select the script variable that you want to change. Expand **DN** and select **Voicemail_gv**.
6. Click **Script Variable Properties**.
7. In the **Script Variable Properties** property sheet, on the **Attribute** tab, change the **Value** field as required. Enter the voice mail number for your solution. The default voice mail number is 6999.

The screenshot shows the Avaya Scripting interface. The left pane displays a system tree with 'Script Variables' expanded under the 'CC' server. The main pane shows a table of 'Script Variables' with columns: Name, Scope, Type, Used in Script, Modified By, and Last Modified. The 'Voicemail_gv' variable is selected. Below the table, the 'Script Variable Properties' dialog box is open, showing the 'Attribute' tab. The 'Type' is set to 'DN' and the 'Value' is '123456'. The 'Class' is set to 'Item'.

Name	Scope	Type	Used in Script	Modified By	Last Modified
CC_INITDNMAIL	Global	DN	No	Installer, CCDS	6/30/2015 8:52:58 AM
sce_dn1	Call	DN	No	Administrator, Web	11/4/2008 1:46:11 PM
varsdn	Call	DN	No	Installer, CCDS	6/30/2015 8:52:58 AM
Voicemail_gv	Global	DN	Yes	Web, Administrator	6/30/2015 8:55:19 AM

8. Click **Submit**.

Changing the voice prompt audio files

Before you begin

- Record your own media files. Avaya Contact Center Select provides optimum playback performance with .WAV files encoded as Linear 16-bit PCM, 8KHz Mono with a bit rate of 128kbits/sec.
- Copy the media files onto the Avaya Contact Center Select server.

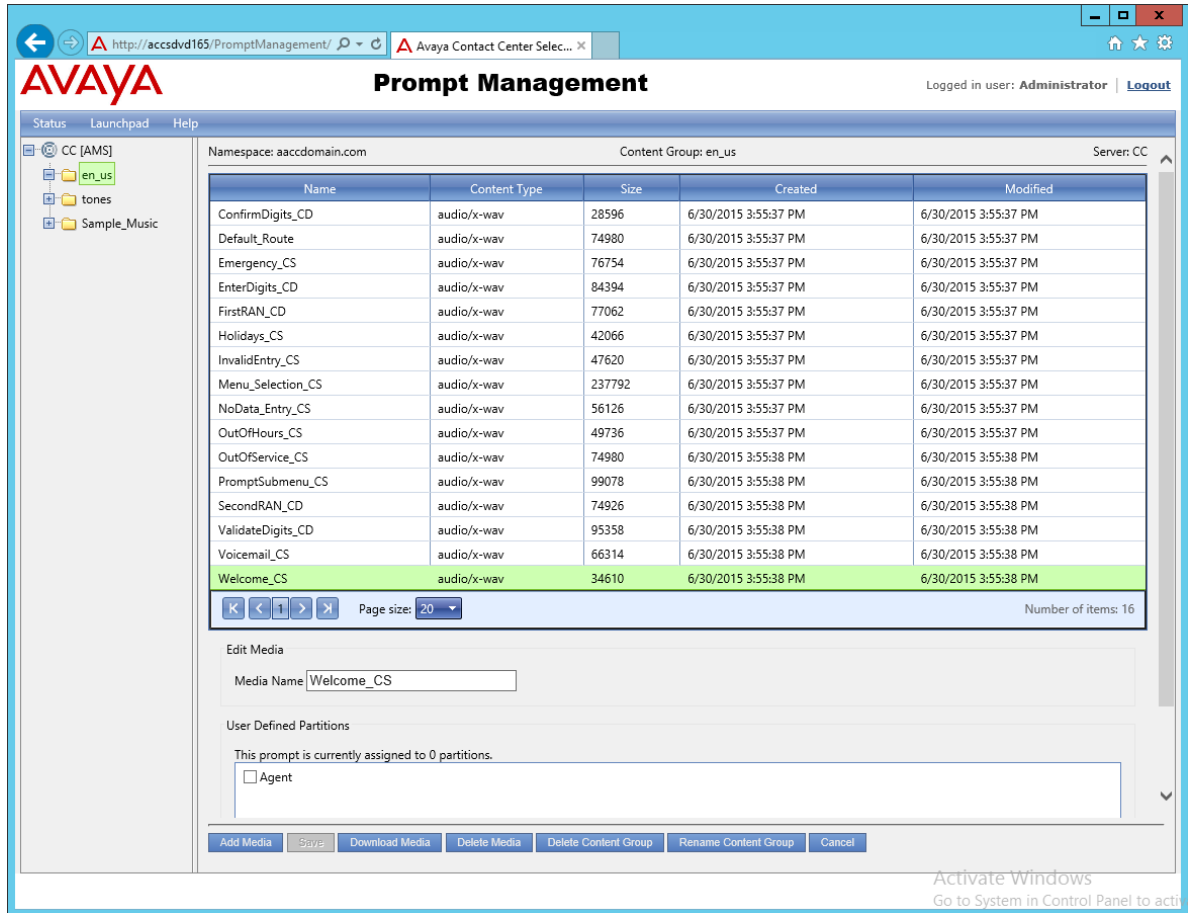
About this task

Avaya Contact Center Select provides a number of default media files. You can replace these default media files with your own recordings.

For example, to replace the Welcome_CS media file, record your own main welcome audio media file, and add the media file to the Avaya Contact Center Select Content Group, giving it a *Media Name* of Welcome_CS.

Procedure

1. Start Internet Explorer.
2. In the **Address** box, type the URL of the Avaya Contact Center Select server. The default URL is `http://<server name>`, where `<server name>` is the computer name of the Avaya Contact Center Select server.
3. Press **Enter**.
4. In the main logon window, in the **User ID** box, type the user name.
5. In the **Password** box, type the password.
6. Click **Log In**.
7. From the **Launchpad**, select **Prompt Management**.
8. In the Prompt Management window, in the left pane, expand the system tree.
9. In the left pane, expand the locale-specific Content Group for your solution. For example, expand **en_us**.



10. In the right pane, select the audio media file to update. Note the Name of the media. For example, note "Welcome_CS".
11. Click **Add Media**.
12. Click **Select** and browse to the location of your custom audio media file.
13. Click **Open**.
14. In the **Media Name** box, type the name of the existing media that you want to replace. For example, type Welcome_CS.
15. Click **Save**.
16. On the message box, click **OK** to overwrite the existing media file.

Chapter 18: Avaya Contact Center Select users

Avaya Contact Center Select includes two types of users in Contact Center Manager Administration — an administrator user and a supervisor user. By default, Contact Center creates one administrator user and two supervisor users. Contact Center assigns the appropriate access classes and partitions to the created accounts.

A supervisor user can perform only a subset of the tasks an administrator can perform. This includes, but is not limited to:

- assigning agents to skillsets
- changing an agent's supervisor
- creating and editing activity codes
- viewing existing real-time reports
- making private copies of real-time reports
- launching Emergency Help
- running historical reports
- using the Audit Trail

The Launchpad options available to a supervisor user in Contact Center Manager Administration are limited. The administrator can choose to edit the access classes and partitions assigned to a supervisor user.

The administrator performs advanced configuration tasks in Contact Center Manager Administration, in addition to the tasks listed above.

The *Sample Agent Starting ID* default value is 6001. The default *Number of sample agents to create* is 10.

The default users and supervisors all have the same default password. This default password is configured on the *Sample Data* tab of the Avaya Contact Center Select Ignition Wizard during deployment.

Logging on to Contact Center Manager Administration

Before you begin

- Ensure the client computer meets the administration client computer requirements. For more information, see *Avaya Contact Center Select Solution Description*.
- Configure Internet Explorer. For more information, see [Configuring Internet Explorer](#) on page 232.

About this task

Log on to Contact Center Manager Administration (CCMA) to configure and administer your contact center resources.

You can log on to CCMA for the first time as an administrator or a supervisor. For security reasons, Avaya recommends that you change the default password when you first log on to the application. CCMA user passwords can contain only English characters and special characters.

Procedure

1. Start Internet Explorer.
2. In the **Address** box, type the URL of the Avaya Contact Center Select server. The default URL is `http://<server name>`, where `<server name>` is the host name of the Avaya Contact Center Select server.
3. Press **Enter**.
4. In the main logon window, in the **User ID** box, type the user name. The default user ID is Administrator.
5. In the **Password** box, type the password. The default user password is Administrator.
6. Click **Log In**.

Contact Center Manager Administration (CCMA) displays your previous CCMA login information and also the number of failed login attempts before a successful login.

Creating a new agent

Before you begin

- Log on to Contact Center Manager Administration (CCMA).
- If you want to associate an agent with a domain account, you must first add the server to the domain.


About this task

Complete this procedure to use Contact Center Manager Administration to create a new Avaya Contact Center Select agent. Contact Center Manager Administration also uses the agent's name and password to create a local Windows account on the Avaya Contact Center Select server.

Procedure

1. On the Contact Center Manager Administration **Launchpad**, select **Contact Center Management**.
2. In the left pane, click the Contact Center Manager Server under which to add the agent.
3. From the **Add** menu, select **Agent**.
4. In the New Agent Details window, enter the following mandatory information about the agent:
 - First name
 - Last name
 - Login ID
 - Primary supervisor
 - Password
 - Confirm Password
5. Enter any optional information about the agent (for example, Call Presentation Class, Threshold, Title, Department, or Comments).
6. Under **Windows User Account Details**, select **Workgroup** or **Domain**. If your solution implements the Business Continuity feature, the **Domain** option is available.
7. If you select **Workgroup**:
 - a. In the **Password** box, type the password for the new local Windows user account associated with this agent.
 - b. In the **Confirm Password** box, retype the password.
8. If you select **Domain**:

In the **User name** box, type the name of the agent's domain user account in the format DomainName\UserAccountName. This domain account is associated with the agent.

 **Important:**

You must ensure that you associate the agent with a correct and valid domain user account.
9. If this agent uses the multiplicity feature on Agent Desktop, select a multiplicity presentation class from the **Multiplicity Presentation Class** list.

If multiplicity is not enabled, the Multiplicity Presentation Class list does not appear.
10. Click the **Contact Types** heading.
11. Select the check box beside each **Contact Type** to assign that contact type to the agent.
12. Click the **Skillsets** heading.
13. Click **Assign Skillsets**.

14. Click **List All** to list all skillsets configured on the server.
15. From the **Priority** list for each skillset to assign to the agent, select the priority level or select **Standby** to put the agent in standby mode for this skillset.
 Priority levels range from 1 to 48, with 1 being the highest priority for the skillset.
16. Select the check boxes beside the partitions to which to add the new agent.
17. Click **Submit** to save your changes.

Agent variable definitions

Name	Description
First Name	The first name of the user. The first name is mandatory for all users and can be a maximum of 30 characters long.
Last Name	The last name of the user. The last name is mandatory for all users and can be a maximum of 30 characters long.
Title	The title for the user. The title is optional and can be up to 40 characters long.
Department	The user's department. The department is optional and can be up to 40 characters long.
Language	Select the language preference for the user. Language selection is mandatory for all users.
Comment	Comments you have about the user. Comments are optional and can be up to 127 characters in length.
User Type	Select the user type. This value is mandatory. Select the agent user type. Agents are users who are assigned skillsets and who answer contacts in the Contact Center. All agents must be assigned to a supervisor.
Login ID	The number that the user enters to log on to the phone. This value is mandatory for all users.
Windows User Account Details — Password (Workgroup only)	Contact Center Manager Administration uses the agent name and password to create a local Microsoft Windows user account on the Avaya Contact Center Select server. Enter a suitably complex password for the agent's Microsoft Windows user account.

Table continues...

Name	Description
Windows User Account Details — User name (Domain only)	<p>The existing domain user account to associate with the agent, in the format DomainName \UserName.</p> <p>The account details must be correct. Agents cannot log on to Agent Desktop if you type the account details incorrectly.</p>
Primary Supervisor	<p>The agent's supervisor. You can choose from all supervisors configured on the server to which you are currently logged on.</p>
Call Presentation	<p>The call presentation class to assign to this agent. The call presentation class determines whether the agent can take a break between calls, whether the agent can put DN calls on hold for incoming ACD calls, and whether the agent phone shows that the agent is reserved for a network call.</p> <p>Call Presentation is mandatory for all users with agent and supervisor/agent capability.</p>
Multiplicity Presentation Class	<p>The multiplicity presentation class to assign to this agent. The multiplicity presentation class determines the type and number of Multimedia contacts an agent can have open simultaneously on Agent Desktop.</p> <p>If multiplicity is not enabled, the Multiplicity Presentation Class list does not appear.</p>
Threshold	<p>The threshold class to assign to this user.</p> <p>The threshold class is mandatory for all users with agent and supervisor/agent capability.</p>

Updating agent details

Before you begin

- Log on to Contact Center Manager Administration (CCMA). For more information, see [Logging on to Contact Center Manager Administration](#) on page 256.

About this task

Complete this procedure to edit the details of an agent or supervisor/agent.

Procedure

1. On the Contact Center Manager Administration **Launchpad**, select **Contact Center Management**.
2. From the **View/Edit** menu, select **Supervisors**.

3. In the left pane, click the server on which to work with the supervisor/agent profile.
The list of supervisors configured on the server appears.
4. Click the supervisor to whom the agent is assigned.
The tree expands to show the list of agents assigned to this supervisor.
5. Right-click the agent whose profile you want to edit, and then select **View Agent Details**.
6. On the Supervisor/Agent Details window, in the **User Details** and **Agent Information** sections, you can change agent details, such as first name, last name, user type, phone login ID, primary supervisor, call presentation, threshold, title, department, or comments.
7. To change the current skillset assignment or assign the agent to new skillsets, click the **Skillsets** heading.
The list of currently assigned skillsets appears.
8. To change the priority level for a skillset, in the table of assigned skillsets, from the **Priority** list, select a new priority level.
9. To assign the agent to new skillsets, click **List All** to list all skillsets configured on the server.
10. In the table listing all skillsets, from the **Priority** list, select the priority level for each skillsets to which you want to assign the agent.
OR
Select Standby to put the agent in standby mode for this skillset.
Skillset priority levels range from 1 to 48, with 1 being the highest priority for this skillset.
11. Select the check box for each partition to which you want to add the agent.
12. Click **Submit** to save your changes.

Copying agent properties

Before you begin

- Log on to Contact Center Manager Administration (CCMA). For more information, see [Logging on to Contact Center Manager Administration](#) on page 256.

About this task

There are several ways to copy an agent's properties. This procedure lists one possible way. You can also click Copy Agent Properties on the Functions menu in the Agents List window, or you can right-click an agent name in the system tree, and then click Create Copy from the resulting pop-up menu.

You can create new agents quickly by copying the properties of existing agents. New agents assume the following properties from the existing agent:

- Skillset assignment
- Department
- User type
- Language
- Comment
- Supervisor
- Call presentation
- Threshold
- Contact type

When you copy an agent's properties, you must type in the new agent's name, login ID, and password.

Procedure

1. On the Contact Center Manager Administration **Launchpad**, select **Contact Center Management**.
2. From the **View/Edit** menu, select **Supervisors**.
3. In the left pane, click the server containing the agent to copy.
4. In the left pane, click the agent's supervisor.

The Supervisor window appears in the right pane, listing the assigned agents in a table.

5. In the table, right-click on the agent to copy, and then select **Copy Agent Properties**.

The agent's properties appear in the New Agent Details window.

6. In the **User Details** section, type the new agent's name and phone login ID.
7. Optionally, can also change any of the copied properties. For example, you can assign the agent to new skillsets or partitions in the appropriate areas of this window.
8. After you configure the new agent, click **Submit** to save the agent under the specified supervisor.

The agent's icon appears in the system tree.

Part 8: Agent Desktop

Chapter 19: Agent Desktop software installation

This section describes how to install Agent Desktop software using the ClickOnce deployment method or using an MSI file.

Avaya Contact Center Select agents can use the ClickOnce deployment method to download and install Agent Desktop client software from the Avaya Contact Center Select server.

Avaya Contact Center Select administrators can use the MSI file deployment method to push Agent Desktop software to agent client computers using a silent install.

If your solution uses the Avaya Contact Center Select Business Continuity feature, verify that the solution is functional and resilient before installing Agent Desktop software on all of the client computers.

Contact Center supports backwards compatibility with the previous Feature Pack or Service Pack version of Agent Desktop. This allows you to upgrade the Contact Center server without the requirement to upgrade Agent Desktop in a single maintenance window. For example, if you upgrade to Release 7.0 Feature Pack 3, you can use the Release 7.0 Feature Pack 2 version of Agent Desktop. New Agent Desktop features added in the latest Contact Center release are not available until you upgrade Agent Desktop to that release.

Backwards compatibility is not supported for major or minor releases. For example, if you upgrade to Release 7.1, you cannot use the Release 7.0 version of Agent Desktop.

Installing Agent Desktop software using ClickOnce

Before you begin

- Ensure the client computer meets the hardware and networking requirements for Agent Desktop software. For more information about Agent Desktop requirements, see *Avaya Contact Center Select Solution Description*.
- Ensure the client computer meets the Operating System requirements for Agent Desktop software. For more information about Agent Desktop requirements, see *Avaya Contact Center Select Solution Description*.

About this task

Install Agent Desktop software to handle Avaya Contact Center Select customer contacts.

Procedure

1. In Windows Explorer, Internet Explorer or Microsoft Edge, type the HTTP address (URL) provided by your system administrator.

The URL format is:

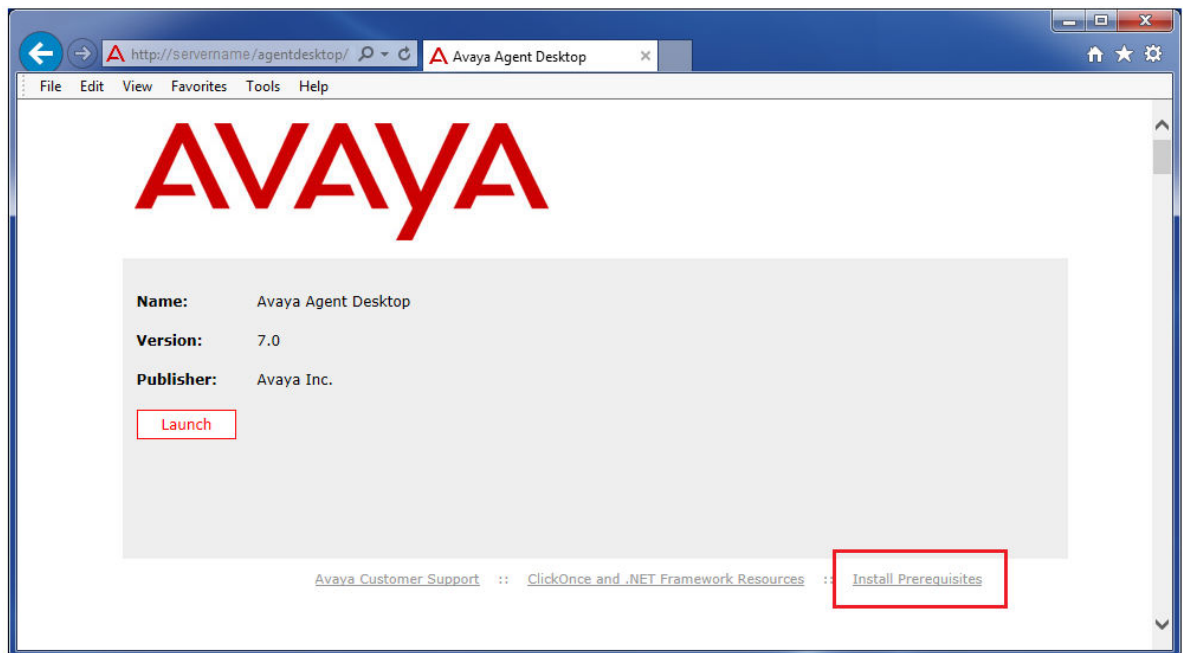
```
http://<ContactCenterServerName>/agentdesktop
```

Where <ContactCenterServerName> is the Avaya Contact Center Select server name.

*** Note:**

The Agent Desktop installer does not use a secure HTTPS connection, even if Web Services security is turned on.

2. Click **Install Prerequisites** and follow the on screen instructions to install the .NET and operating system components required to run Agent Desktop software.



3. Click **Launch** to download and install the most recent version of Agent Desktop software.

Agent Desktop client software silent installation

This section describes how to install the Agent Desktop client software silently, using an MSI file, on each client computer in your contact center. Avaya Contact Center Select agents use Agent Desktop software to handle customer voice and multimedia contacts.

! Important:

Avaya Contact Center Select does not support the softphone integrated in the Avaya Agent Desktop MSI installation package. When installing Avaya Agent Desktop using the MSI file, disable this softphone option.

Installing software prerequisites for an Agent Desktop silent install

Before you begin

- Download the most recent Service Pack and patches from the Avaya support website, <http://support.avaya.com>.

About this task

Install the software prerequisites for Agent Desktop, so that you can install Agent Desktop silently. You can use the Windows Add\Remove programs utility to uninstall the Agent Desktop software prerequisites.

Procedure

1. Log on to the Avaya Contact Center Select server using administrator privileges.
2. Browse to <Drive>:\Avaya-ProductUpdates\Install Software\CCMM \AvayaCC_CCMM_<XXX>\AAAD Prerequisites, where <Drive> is the drive containing the most recent Service Pack, and <XXX> is the version number of the latest Service Pack.
3. Copy the prerequisites folder to a location from which you can copy it to the client computer.

For example, copy the AAAD Prerequisites folder to a USB memory stick or network location.
4. Log on to the client computer using administrator privileges.
5. Copy the prerequisites folder to the client computer.
6. Install Microsoft .NET Framework 4.6.2. When you install Microsoft .NET Framework 4.6.2, you also get .NET Framework 4.0 and 4.5.

Installing Agent Desktop client software silently

Before you begin

- Download the most recent Service Pack and patches from the Avaya support website.

About this task

Install Agent Desktop client software silently to install the software as a desktop application with an All Users profile. This allows all agents that can log on to the client computer to run Agent Desktop software. By default, the Agent Desktop software installs in the Program Files folder.

Important:

Avaya Contact Center Select does not support the softphone integrated in the Avaya Agent Desktop MSI installation package. When installing Avaya Agent Desktop using the MSI file, disable this softphone option.

You can use the Windows Add\Remove programs utility to uninstall the Agent Desktop software.

Procedure

1. Log on to the Avaya Contact Center Select server using administrator privileges.
2. Browse to <Application Drive>:\Avaya\Contact Center\Multimedia Server\Agent Desktop\Client\, where <Application Drive> is the drive on which you installed Avaya Contact Center Select software. By default, this is the D: drive.
3. Copy the AvayaAgentDesktopClient.msi installation file to a USB memory stick or network location.
4. Log on to the client computer using administrator privileges.
5. Copy the AvayaAgentDesktopClient.msi installation file to the client computer.
6. Open a command prompt by clicking **Start > All Programs > Run**. Type **cmd** and press Enter.
7. Use the Microsoft Windows Installer program (msiexec.exe) to install the software. For example:

```
C:\AAAD>msiexec.exe /package AvayaAgentDesktopClient.msi /
quiet /log "products.log" AAADSOFTPHONE=0
MMSERVERNAME=MyCCMMServer AAADUSEHTTPS=FALSE
```

Where:

- AAADSOFTPHONE — Avaya Contact Center Select does not support the Agent Desktop integrated softphone. Set this parameter to 0.
- MMSERVERNAME — This parameter configures the name of the Avaya Contact Center Select server that the Agent Desktop application communicates with. This parameter can be an IP Address or a server name.
- AAADUSEHTTPS — This binary parameter (TRUE or FALSE) configures Agent Desktop to communicate with the Avaya Contact Center Select server using Hypertext Transfer Protocol Secure (HTTPS). The default value is FALSE, do not use HTTPS.

The Agent Desktop software installs silently.

8. Close the command prompt window.

Part 9: Reporting

Chapter 20: Real Time Reporting

The Contact Center Manager Administration (CCMA) Real-Time Reporting displays provide up-to-date statistics for your contact center and resources. With access to statistics that update in real-time, such as the number of contacts waiting to be answered, the number of agents assigned to each skillset, and the number of abandoned calls, you can view changes in contact activity as they occur.

Real-time data is presented in the best format to help you react immediately to changing circumstances, adjust skillsets and staffing levels, or reroute calls to other resources. Real-Time Reporting displays make it easy to monitor peak periods and then adjust staffing levels as appropriate - all to maintain the highest levels of customer service.

Using the Contact Center Status real-time display

About this task

Use the Avaya Contact Center Select Real-Time Reporting displays to monitor the performance of the contact center in near real-time.

Avaya Contact Center Select offers a number of default public real-time displays. Create a private copy of these displays and experiment with them to create displays that meet the day-to-day requirements of your business.

For example, the CC Status public graphical display has the following panels:

Panel	Type	Description
CC_Standard_Agent_Display (CC)	Tabular	This tabular panel displays the agent status and time in current state. Use this panel to monitor individual agent activity.
CC_Contacts_Wait	Chart	This pie chart displays the number of contact waiting for each skillset.
CC_Standard_Application_Display	Tabular	This tabular panel displays the maximum wait times, and the number of contacts offered, waiting, answered, or abandoned.
CC_Sample_Skills	Chart	This panel displays the service level for each skillset.

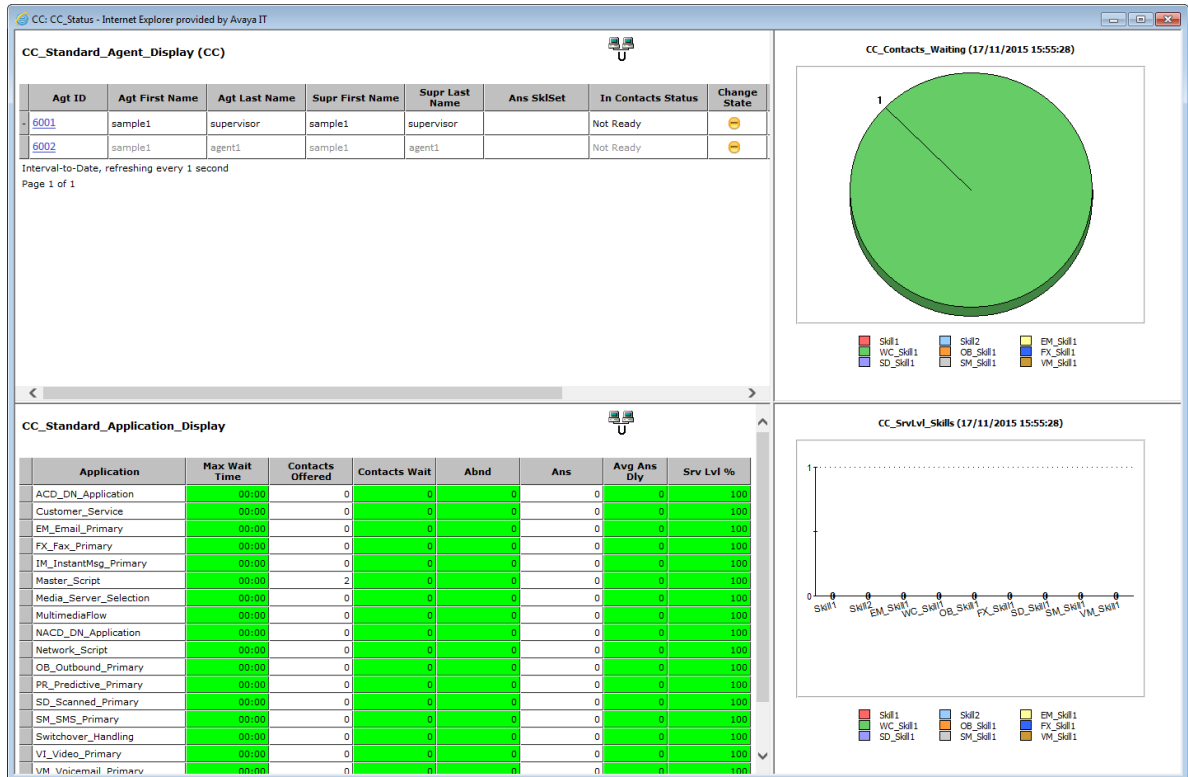
This combined display provides a real-time status report about important Avaya Contact Center Select performance parameters.

Procedure

1. Start Internet Explorer.
2. In the **Address** box, type the URL of the Avaya Contact Center Select server. The default URL is `http://<server name>`, where `<server name>` is the computer name of the Avaya Contact Center Select server.
3. Press **Enter**.
4. In the main logon window, in the **User ID** box, type the user name. The default user ID is Administrator.
5. In the **Password** box, type the password. The default user password is Administrator.
6. Click **Log In**.
7. On the Contact Center Manager Administration **Launchpad**, click **Real-Time Reporting**.
8. In the left pane, select the **Public Graphical Displays** folder.
9. In the left pane, from the list of displays, select **CC_Status**.
10. On the **Public Collection properties** tab, select the default display options for CC Status. These standard displays combine to form an effective Real-Time Reporting graphical display.
11. On the **Public Collection properties** tab, click **Launch**.

The Contact Center Status real-time display appears. The values you see on your display depend on the number of active agents and contacts in your solution.

Real Time Reporting



12. Use the display to monitor contact center performance in near real-time. Use this information to tune the contact center to changing circumstances, adjust skillsets and staffing levels, or reroute calls to other resources.
13. For more information about creating a private and modifiable copy of this real-time display, see *Administering Avaya Contact Center Select*.
14. Experiment with Real-Time Reporting to find, copy, or create a set of displays that meet the day-to-day requirements of your solution.

Part 10: Troubleshooting

Chapter 21: Troubleshooting tips

This section describes how to troubleshoot Avaya Contact Center Select. To avoid the frustration of troubleshooting; plan your solution in advance. You can troubleshoot problems better by planning for events in advance and having up-to-date information if troubleshooting is required. For example, ensure that you know the correct user accounts, passwords, solution resources, and network details. Plan ahead and ensure that you are using the correct information to install and commission the Avaya Contact Center Select solution.

The main stages of the troubleshooting process are:

1. Identify the problem. Describe the symptoms of the problem. Is the problem intermittent or reproducible? Has the problem always existed, or was it introduced after a recent configuration change?
2. Determine the cause of the problem. Determining the most likely cause is a process of elimination - eliminating potential causes of a problem. The most likely cause of a problem is misconfiguration. Begin your investigation by double-checking the solution configuration data.
3. Solve the problem. Identify and test the solution to the problem. Intermittent problems require additional and prolonged soak testing.

Begin your troubleshooting by double-checking the solution configuration details, and then verify that the individual components are working. If you are not able to solve the problem, collect all the relevant information and have it available before contacting Avaya Technical Support.

Misconfiguration

In an integrated Avaya Contact Center Select and IP Office solution, the most likely cause of a malfunction is misconfiguration. Avaya Contact Center Select and IP Office must be configured correctly to work with each other. An apparently minor configuration error can be time-consuming and frustrating to resolve. When configuring a solution, plan ahead and proceed with care.

If you encounter an issue with your solution, begin your investigation by double-checking the solution configuration, focusing your investigation on the points of integration between Avaya Contact Center Select and IP Office. Look for mismatched configuration data between Avaya Contact Center Select and IP Office. For example, if IP Office is configured to use CDN (Route Point) 7000, when Avaya Contact Center Select is configured to use CDN (Route Point) 3000. Both must be configured to use the same CDN (Route Point) number. Ensure Avaya Contact Center Select and IP Office both use the same SIP domain name.

Solution components

Ensure that the Avaya Contact Center Select server part of the solution is working as intended. Use the procedures in this section to verify that the Avaya Contact Center Select components are running:

- Ensure the Avaya Contact Center Select application services are running.
- Ensure Avaya Contact Center Select can communicate with IP Office.
- Ensure Avaya Contact Center Select is registered with IP Office.
- Ensure Avaya Contact Center Select is licensed.
- If your solution supports the email contact type, ensure Avaya Contact Center Select can communicate with the email server and mailbox.

Verify that Avaya Contact Center Select is running. If a component is stopped, start it. If the licenses are all used up, obtain more. If email is not working, double-check your email server and mailbox.

Troubleshooting more complex issues

If you are not able to solve the problem, collect all relevant information and have it available before contacting Avaya Technical Support. For all errors, record the error messages, the system configuration, and actions taken before and after the error occurred.

- Review the Avaya Contact Center Select trace log files to diagnose the cause of the errors.
- Review the Avaya Contact Center Select application event logs to diagnose the cause of the errors.

Work with Avaya Technical Support to clearly identify the problem. The Avaya customer support representative might require remote access to Avaya Contact Center Select to complete the investigation.

Troubleshooting by symptom

The following table lists a number of Avaya Contact Center Select issues and suggests a fix for each issue.

Symptom	How to fix
Avaya Contact Center Select services not started	<ul style="list-style-type: none"> • Use the System Control and Monitor Utility to start the services. Click <i>Start Contact Center</i>. • Verify that the most recent Avaya Contact Center Select patches are installed. For more information, see Installing contact center patches on page 222. • Verify the Avaya Contact Center Select server settings are correct using Server Manager > Server Configuration.

Table continues...

Symptom	How to fix
Agents cannot log on to Agent Desktop	<ul style="list-style-type: none"> • Verify that you are using the correct user name and password. The default domain name is the host name of the Avaya Contact Center Select server. • Ensure that there is an available IP Office extension for each Avaya Contact Center Select agent. Ensure the extension is of type H.323. For more information, see Configuring the agent extensions on page 48. • Verify that there are sufficient agent licenses available. For more information, see Checking the Contact Center License Manager real time usage on page 289.
No CTI call control. Agent Desktop is not controlling the agent desk phone.	<ul style="list-style-type: none"> • Verify that Avaya Contact Center Select is communicating with IP Office. For more information, see Checking the Contact Center connection to IP Office on page 288. • Verify that Avaya Contact Center Select is registered with IP Office. For more information, see Checking that the SIP User Extension Number is acquired on IP Office on page 286.
CDN (Route Point) calls not arriving at Avaya Contact Center Select	<ul style="list-style-type: none"> • Verify the IP Office short code number matches the Avaya Contact Center Select CDN (Route Point) number. For more information, see Configuring a shortcode to Contact Center Route Points on page 42. • Verify that there are no space characters in the IP Office short code. • Verify the IP Office short code is configured under the solution node, and not under the IP Office server node. • Verify that the Avaya Contact Center Select CDN (Route Point) number is acquired in Contact Center Manager Administration.
Avaya Contact Center Select not registered in IP Office.	<ul style="list-style-type: none"> • Verify that Avaya Contact Center Select is registered with IP Office as a SIP extension. For more information, see Checking that the SIP User Extension Number is acquired on IP Office on page 286. • Verify that Avaya Contact Center Select is registered as a SIP extension, ensure it is not registered as a H.323 extension.
IP Office calls are routing to the Avaya Contact Center Select CDN (Route Point), but the customer caller cannot hear the welcome announcement.	<ul style="list-style-type: none"> • The IP Office SIP domain name does not match the Avaya Contact Center Select SIP domain name. For more information, see Configuring the SIP domain name on page 40. • The Avaya Aura® Media Server locale setting does not match the Avaya Contact Center Select server locale (country and language) setting.
The Contact Center Manager Administration Web interface menus are not visible in the left pane	<ul style="list-style-type: none"> • Ensure Internet Explorer is using Compatibility mode. • Ensure the Contact Center Manager Administration Web interface client computer display has a resolution of at least 1024 x 768 pixels.
The Contact Center Manager Administration Web interface looks distorted	<ul style="list-style-type: none"> • Ensure the Contact Center Manager Administration Web interface client computer display has a resolution of at least 1024 x 768 pixels. • Ensure Internet Explorer is using Compatibility mode. • Temporarily disable the Internet Explorer pop-up blocker to allow Contact Center Manager Administration Active X controls and libraries to install.

Table continues...

Symptom	How to fix
The Avaya Contact Center Select users visible in Contact Center Manager Administration are not visible in IP Office.	<ul style="list-style-type: none"> Verify the Contact Center Manager Administration synchronization account details used by IP Office. For more information, see Configuring the synchronization user account on page 35. In Contact Center Manager Administration, on the IP Office server configuration window, click <i>Synchronize</i>.

Starting the Contact Center Dashboard

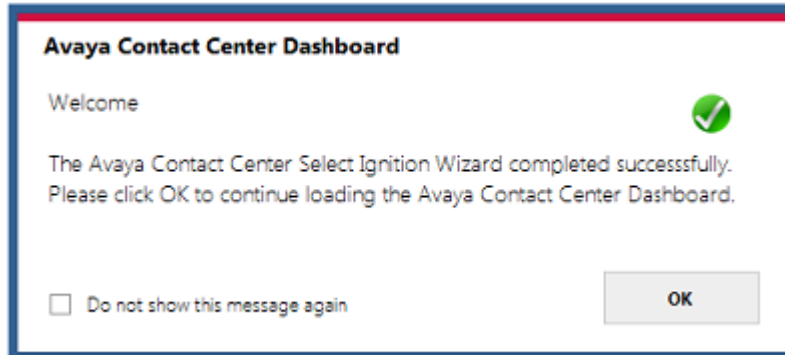
About this task

You can use the Contact Center Dashboard to access Contact Center system tools and diagnose system problems. The Contact Center Dashboard displays some Operating System and system details such as CPU type, network details, and Operating System activation status.

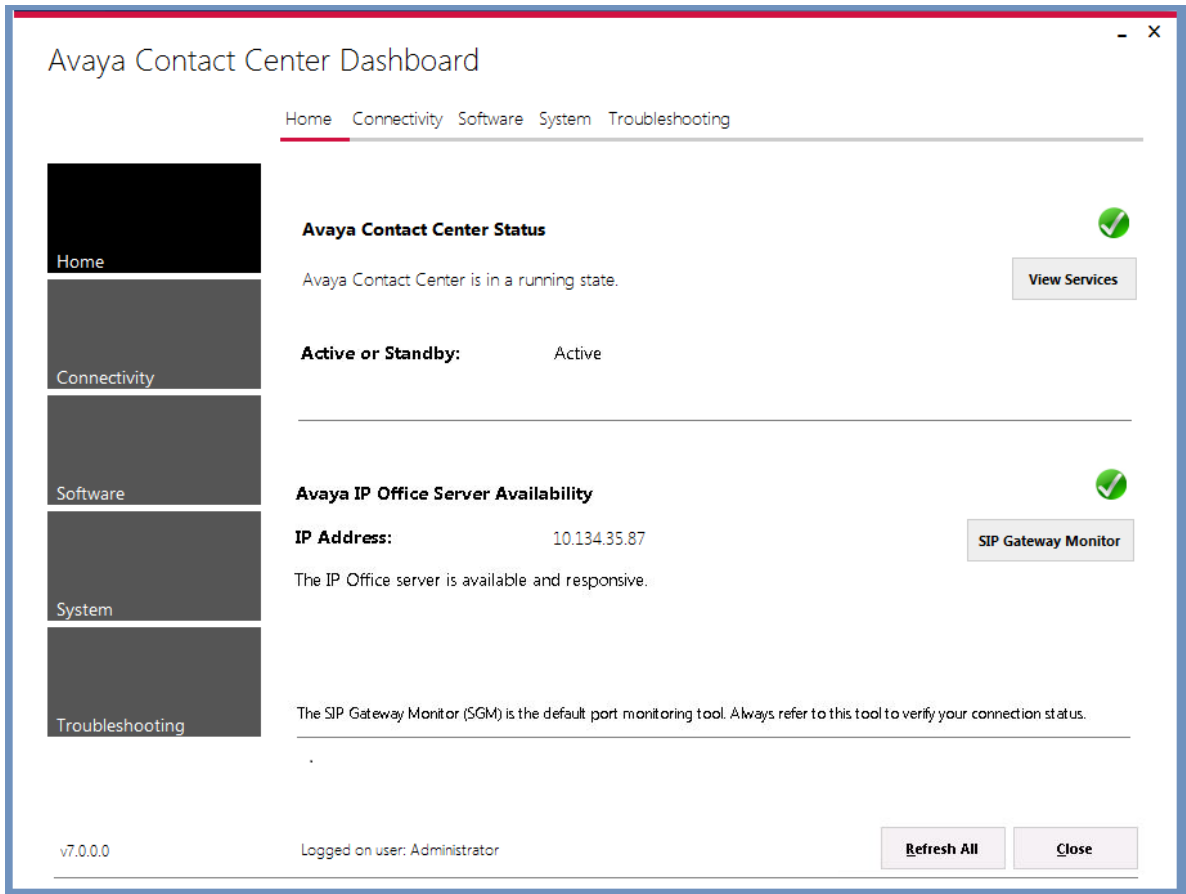
The Contact Center Dashboard launches automatically the first time the Contact Center server boots up.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Contact Center Dashboard**.
2. If the Contact Center Dashboard Welcome message box appears, click **OK**.



3. After a few moments the Contact Center Dashboard appears. Select the **Home** tab.



4. Click **Refresh All** to refresh the Contact Center Dashboard status reports.
5. In the **Avaya Contact Center Status** section, click **View Services** to monitor the state of the Contact Center Windows services.
6. In the **Avaya IP Office Server Availability** section, click **SIP Gateway Monitor** to determine if Contact Center is communicating with IP Office.

7. Select the **Connectivity** tab.

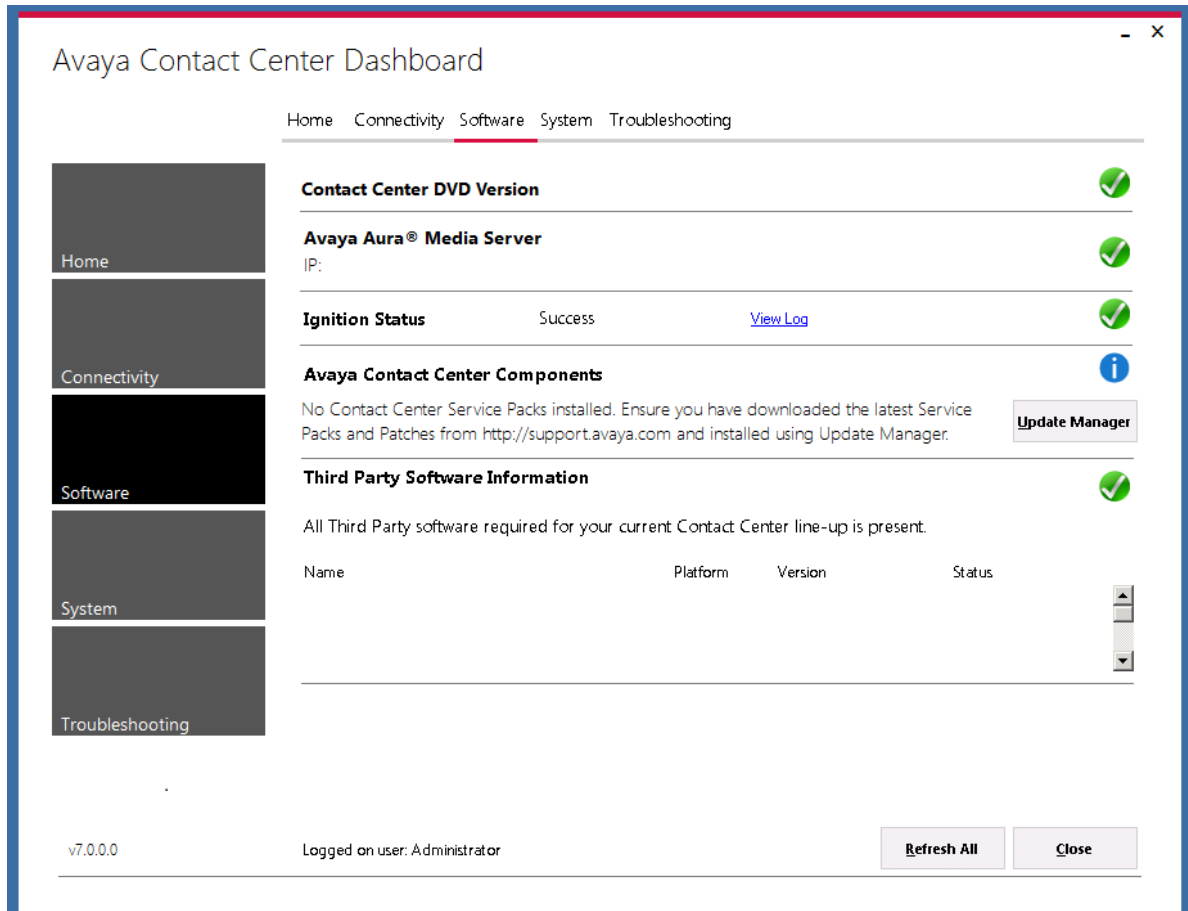
The screenshot shows the Avaya Contact Center Dashboard interface. The title bar reads "Avaya Contact Center Dashboard". Below the title bar is a navigation menu with tabs: Home, Connectivity (selected), Software, System, and Troubleshooting. On the left side, there is a vertical navigation menu with buttons for Home, Connectivity (selected), Software, System, and Troubleshooting. The main content area displays five sections, each with a description and a "Launch" button:

- SIP Gateway Monitor**: Monitor the status of the SIP connection to IP Office. The "Launch" button is highlighted with a red box.
- Contact Center Multimedia Dashboard**: Monitor the multimedia mailbox status.
- Contact Center Manager Administration**: Access Contact Center Manager Administration to configure and manage Contact Center resources.
- System Control and Monitor Utility**: Monitor, stop, and start Contact Center services.
- Contact Center License Manager**: Monitor license status and add additional licensed features.
- Business Continuity Support**: Configure and control Business Continuity support feature for Contact Center.

At the bottom left, the version number "v7.0.0.0" is displayed. At the bottom center, it says "Logged on user: Administrator". At the bottom right, there are two buttons: "Refresh All" and "Close".

8. Select **SIP Gateway Monitor** to monitor the status of the SIP connection to IP Office.
9. Select **Contact Center Multimedia Dashboard** to monitor the multimedia mailbox status.
10. Select **Contact Center Manager Administration** to access Contact Center Manager Administration to configure and manage Contact Center resources.
11. Select **System Control and Monitoring Utility** to monitor, stop, and start Contact Center services.
12. Select **Contact Center License Manager** to monitor license status and add additional licensed features.
13. Select **Business Continuity Support** to configure the Business Continuity feature.

14. Select the **Software** tab.



15. **Contact Center Version** displays the version of the Contact Center software installed on the server.
16. **Avaya Aura® Media Server** displays the version of Avaya Aura® Media Server software installed on the server.
17. **Ignition Status** displays the Contact Center software installation status.
18. **Avaya Contact Center Components** displays the Contact Center software and patch line-up installed on the server.
19. **Third Party Software Information** displays the versions of the third-party software components used by Contact Center that are installed on the server.

20. Select the **System** tab.

Avaya Contact Center Dashboard

Home Connectivity Software **System** Troubleshooting

Machine Name ACCSONE

Windows Domain aaccdomain.com

Operating System Microsoft Windows Server 2012 R2 Standard

Windows Activation Status Activated ✔

RAM 17 % 16384 MB

CPU 1 % 2.926GHz 64bit Intel(R) Xeon(R) CPU X5647 @ 2.93GHz

Network ✔

Name	IP Address	MAC Address
Local Area Connection	10.134.38.1	005056A067

Hard Disks ✔

Name	Volume Name	Total Size GB	Free Space GB	Used
C:\				
D:\				
E:\				
G:\				

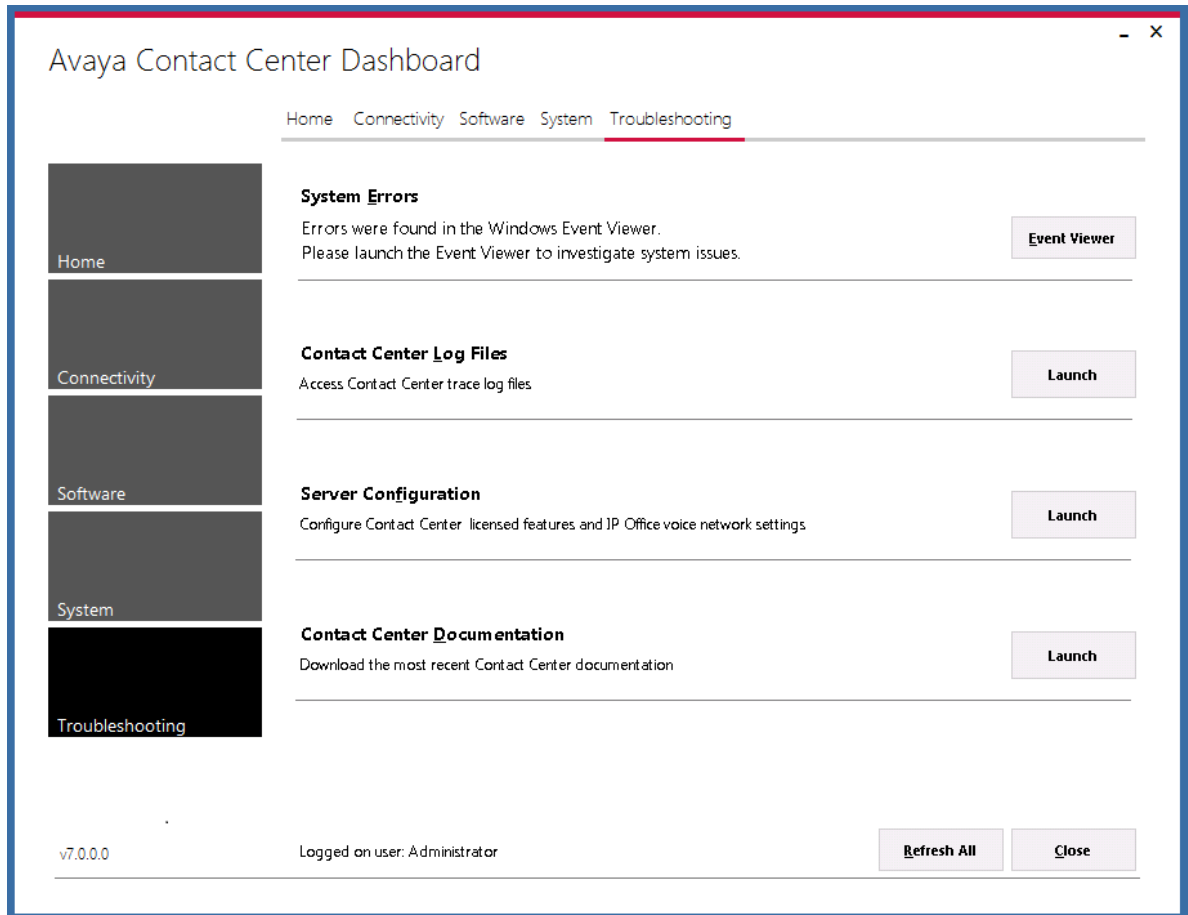
v7.0.0.0

Logged on user: Administrator

Refresh All Close

21. **Machine Name** displays the host name of the Contact Center server.
22. **Windows Domain** displays the name of the domain that the Contact Center server is in.
23. **Operating System** displays the Operating System version.
24. **Windows Activation Status** displays the Windows Operating System license and activation status.
25. **RAM** displays the amount of RAM memory in the server.
26. **CPU** displays the type of CPU in the server.
27. **Network** displays the networking details of the server: IP address and MAC address.
28. **Hard Disks** displays the number, size, and drive letter of the hard disk volumes in the server.

29. Select the **Troubleshooting** tab.



30. Select **System Errors** to access Contact Center events in the Microsoft Windows Event Viewer.
31. Select **Contact Center Log Files** to access Contact Center trace log files.
32. Select **Server Configuration** to configure Contact Center licensed features and IP Office voice network settings.
33. Select **Contact Center Documentation** to access and download the most recent Contact Center documentation from the Avaya support website.

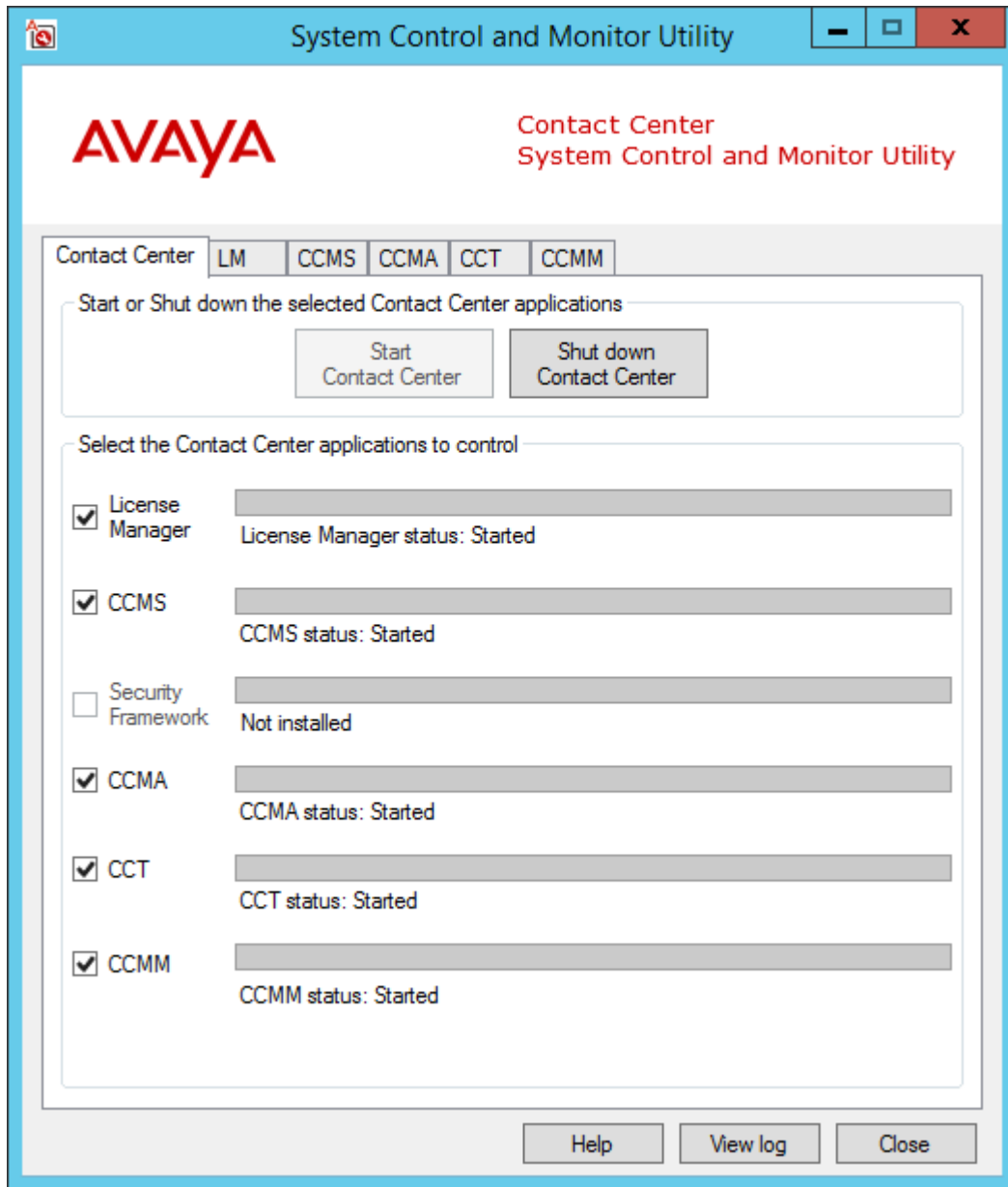
Verifying the Contact Center services are started

About this task

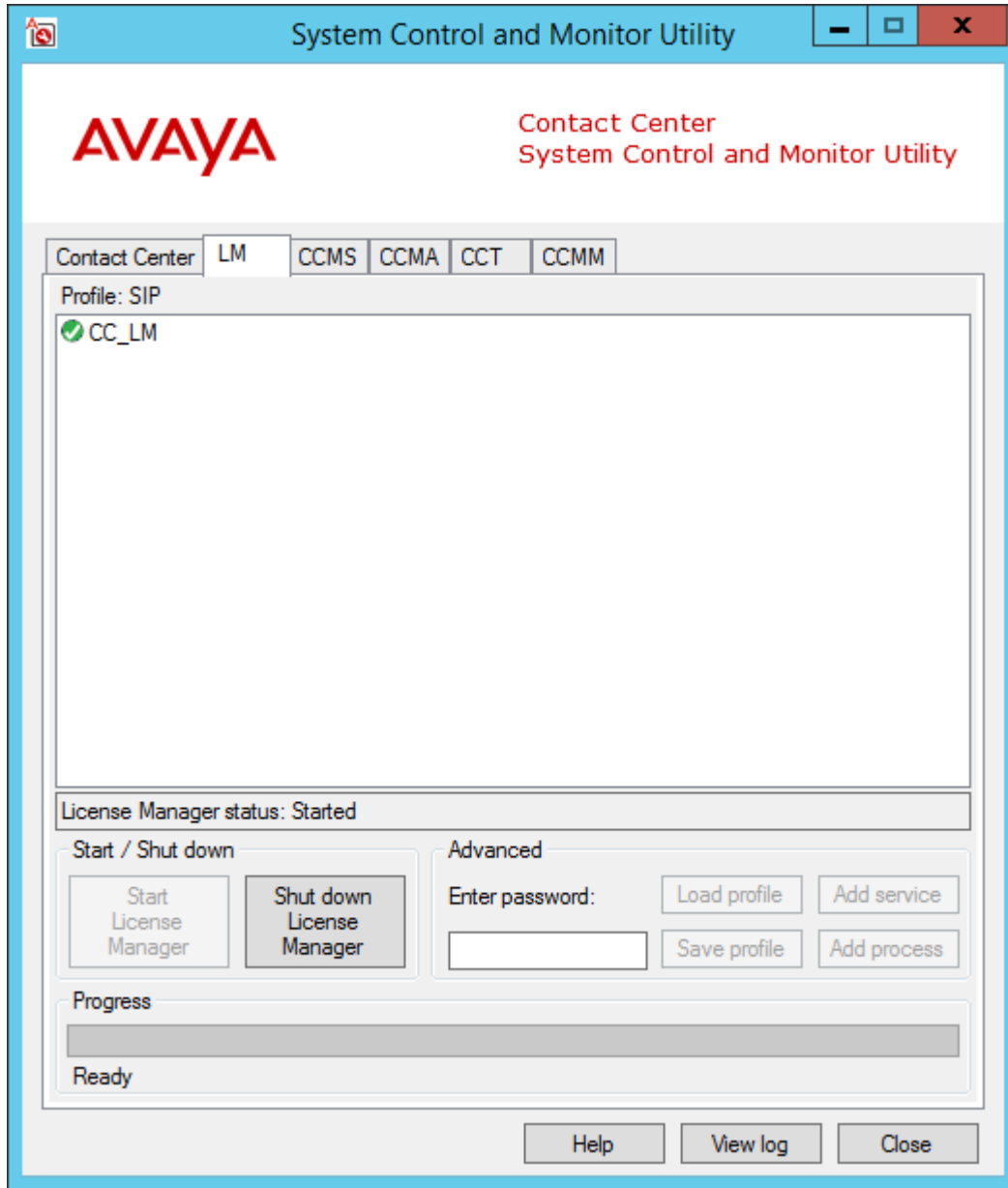
Verify that the Contact Center services are started. Use the System Control and Monitor Utility to verify that all necessary Avaya Contact Center Select services are running.

Procedure

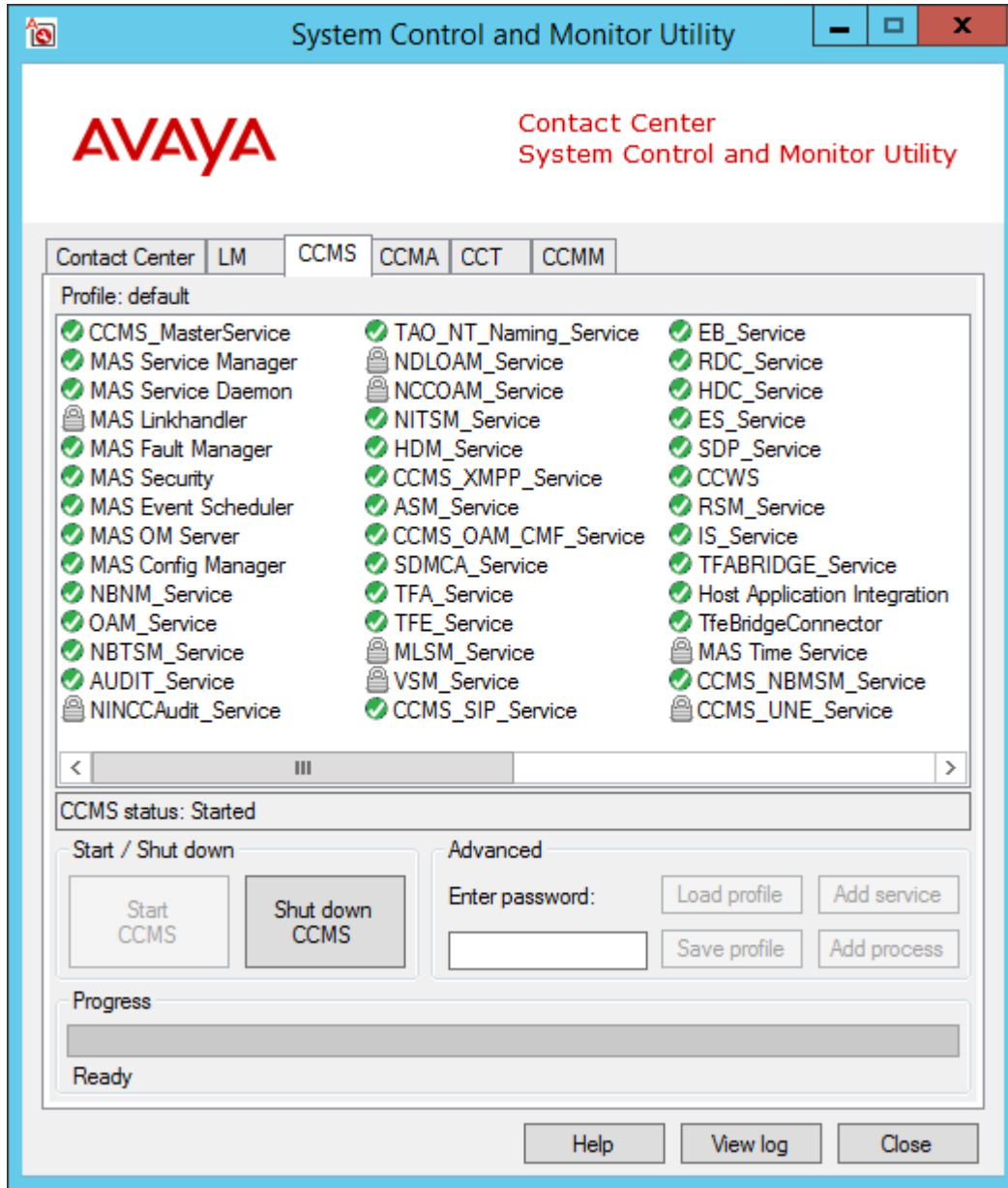
1. Log on to the Avaya Contact Center Select server.
2. On the **Apps** screen, in the **Avaya** section, select **System Control and Monitor Utility**.
3. Click the **Contact Center** tab.



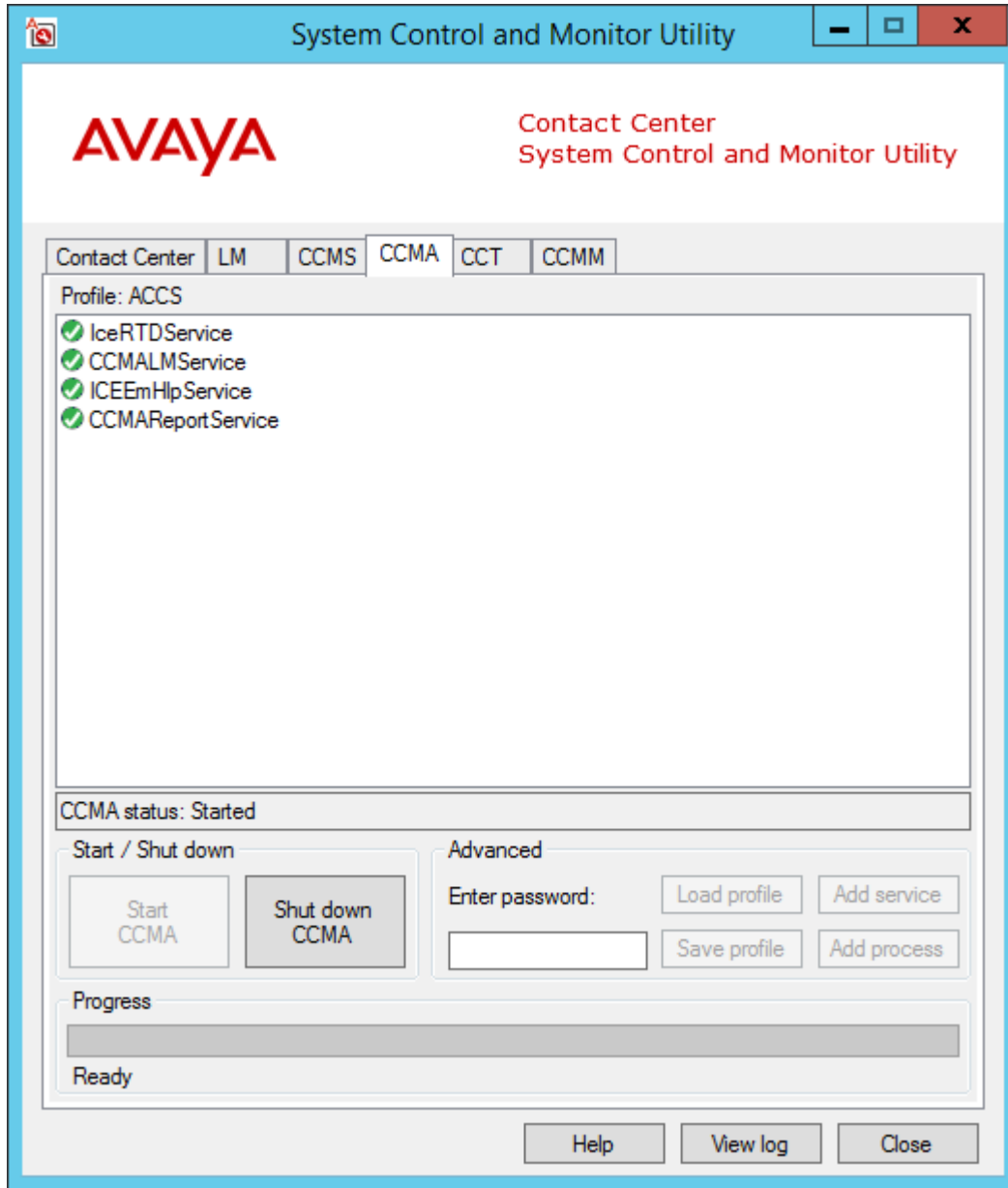
4. Select the **LM** tab, and verify that the Contact Center License Manager service is running.



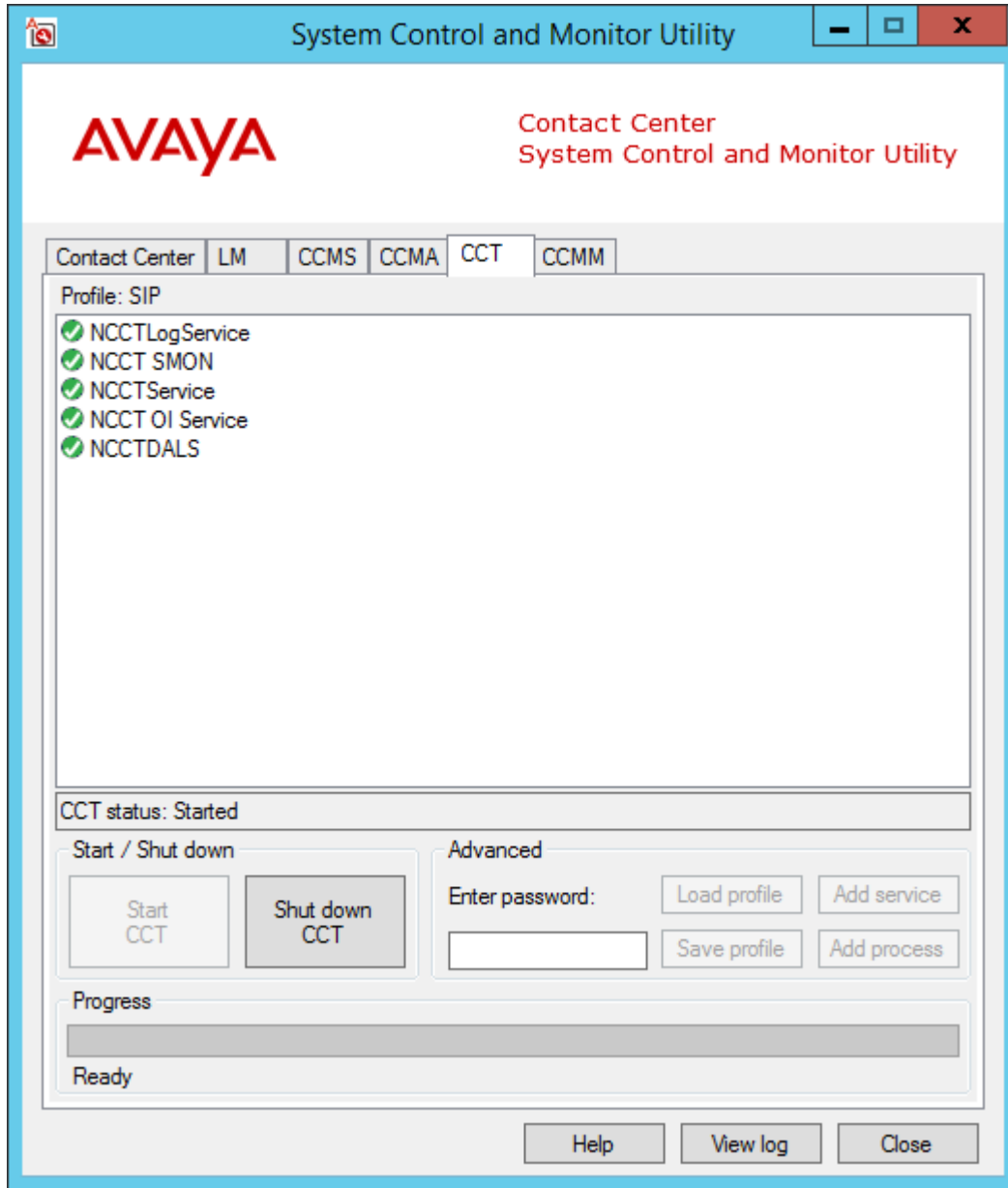
5. Select the **CCMS** tab, and verify that the Contact Center Manager Server services are running.



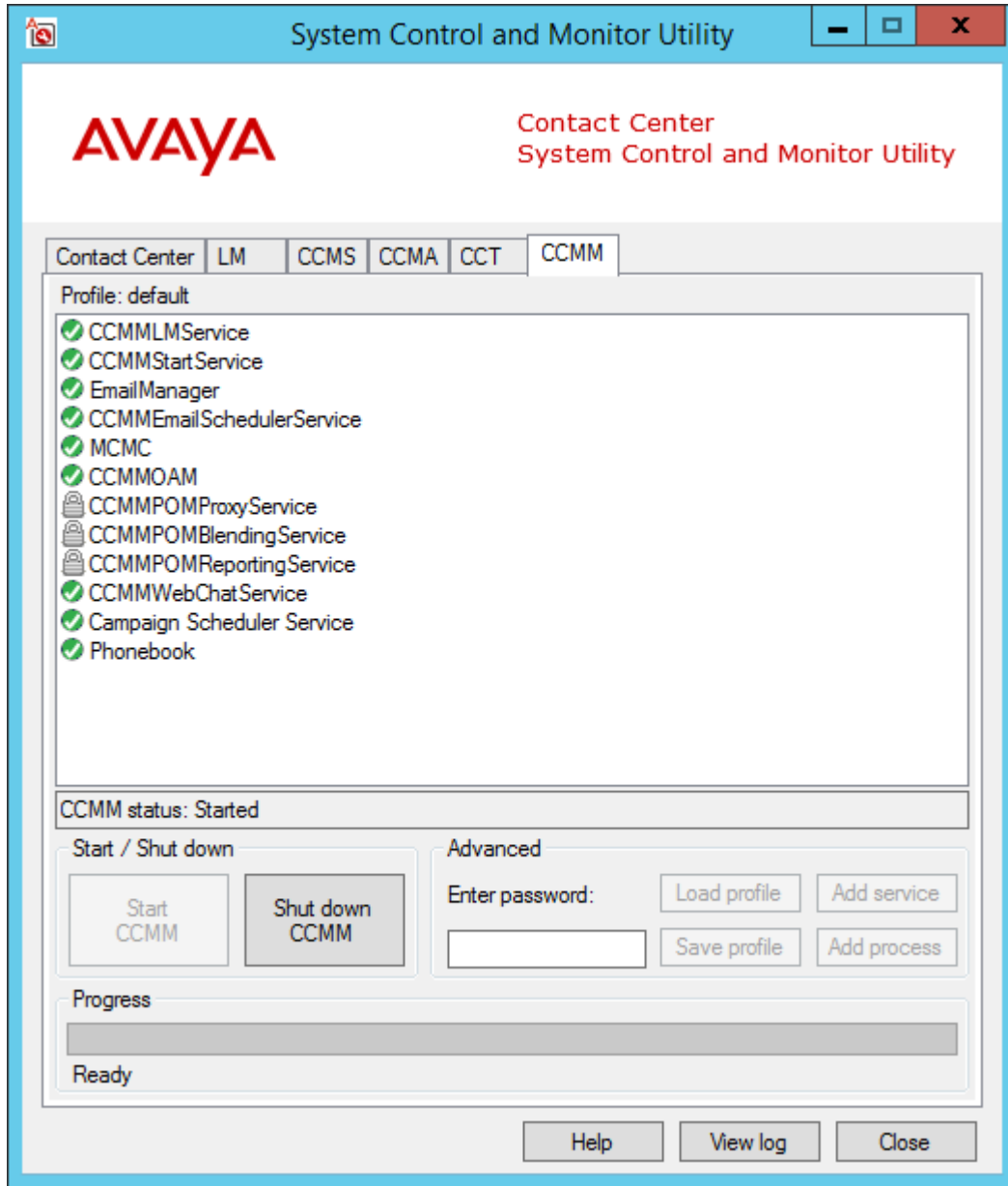
6. Select the **CCMA** tab, and verify that the Contact Center Manager Administration services are running.



7. Select the **CCT** tab, and verify that the Communication Control Toolkit services are running.



8. Select the **CCMM** tab, and verify that the Contact Center Multimedia services are running.



9. Click **Start Contact Center** to start any stopped services.

Checking that the SIP User Extension Number is acquired on IP Office

Before you begin

- Know the IP Office Manager log on details.

- Know how to use IP Office Manager.

About this task

Check that the SIP User Extension Number is acquired on IP Office. Avaya Contact Center Select uses this SIP User Extension Number to register with IP Office for CTI call control and SIP session messaging.

Procedure

1. Using IP Office Manager, select the IP Office server in the **Configuration** pane.
2. In the **Configuration** pane, under the IP Office server, select **User**.
3. Locate the SIP User Extension Number used to register Avaya Contact Center Select.

The screenshot shows the 'User' configuration window in IP Office Manager. The window has several tabs at the top: 'User', 'Voicemail', 'DND', 'ShortCodes', 'Source Numbers', 'Telephony', 'Forwarding', 'Dial In', 'Voice Recording', and 'But'. The 'User' tab is active. The configuration fields are as follows:

- Name: 6000
- Password: [masked]
- Confirm Password: [masked]
- Account Status: Enabled
- Full Name: [empty]
- Extension: 6000
- Email Address: [empty]
- Locale: [dropdown]
- Priority: 5
- System Phone Rights: None
- ACCS Agent Type: None
- Profile: Basic User
- Receptionist:
- Enable Softphone:
- Enable one-X Portal Services:
- Enable one-X TeleCommuter:
- Enable Remote Worker:
- Enable Flare:
- Enable Mobile VoIP Client:
- Send Mobility Email:
- Ex Directory:
- Device Type: Avaya Contact Center Select (highlighted with a red box)
- User Rights: [empty]

At the bottom of the window are three buttons: 'OK', 'Cancel', and 'Help'.

4. If Avaya Contact Center Select is registered with IP Office, the **Device Type** for the SIP User is configured as **Avaya Contact Center Select**.
5. If Avaya Contact Center Select is not registered with IP Office, ensure the SIP User Extension Number and password details in IP Office match the details entered when installing Avaya Contact Center Select.

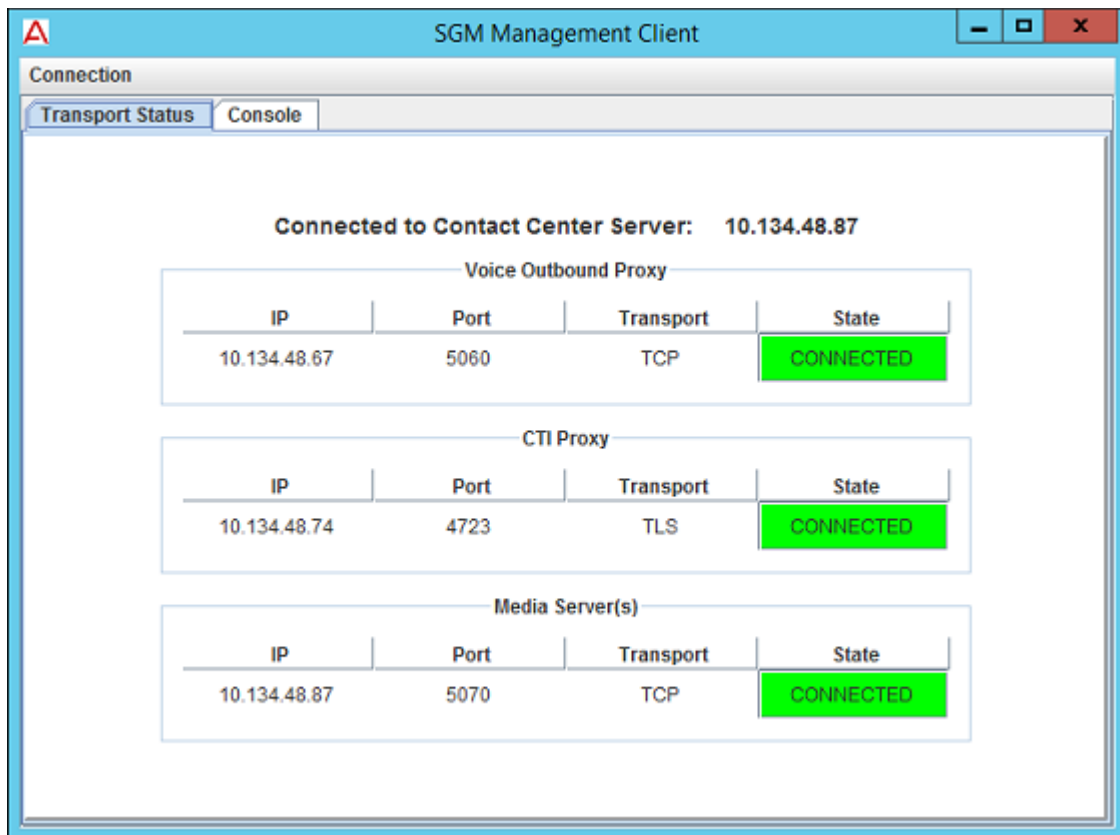
Checking the Contact Center connection to IP Office

About this task

Check the CTI call control and SIP session management connection from Avaya Contact Center Select (ACCS) to IP Office.

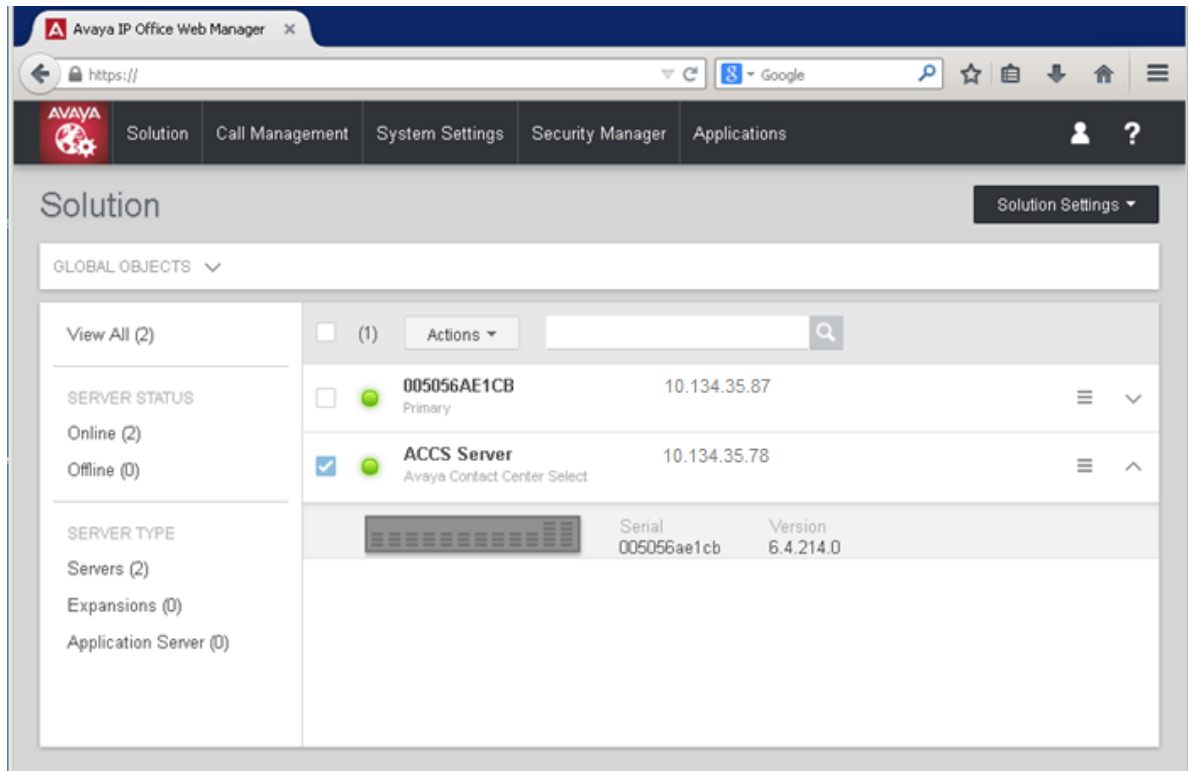
Procedure

1. On the **Apps** screen, in the **Avaya** section, select **SIP Gateway Management Client**.
2. In the **New Connection** window, click **Connect**.



3. Ensure the Voice Outbound Proxy State is **CONNECTED**.
4. Ensure the CTI Proxy State is **CONNECTED**.

5. Log on to IP Office Web Manager and locate the ACCS server in the **Solution** pane. If IP Office is communicating with ACCS, the ACCS server is listed on the **Solution** pane.



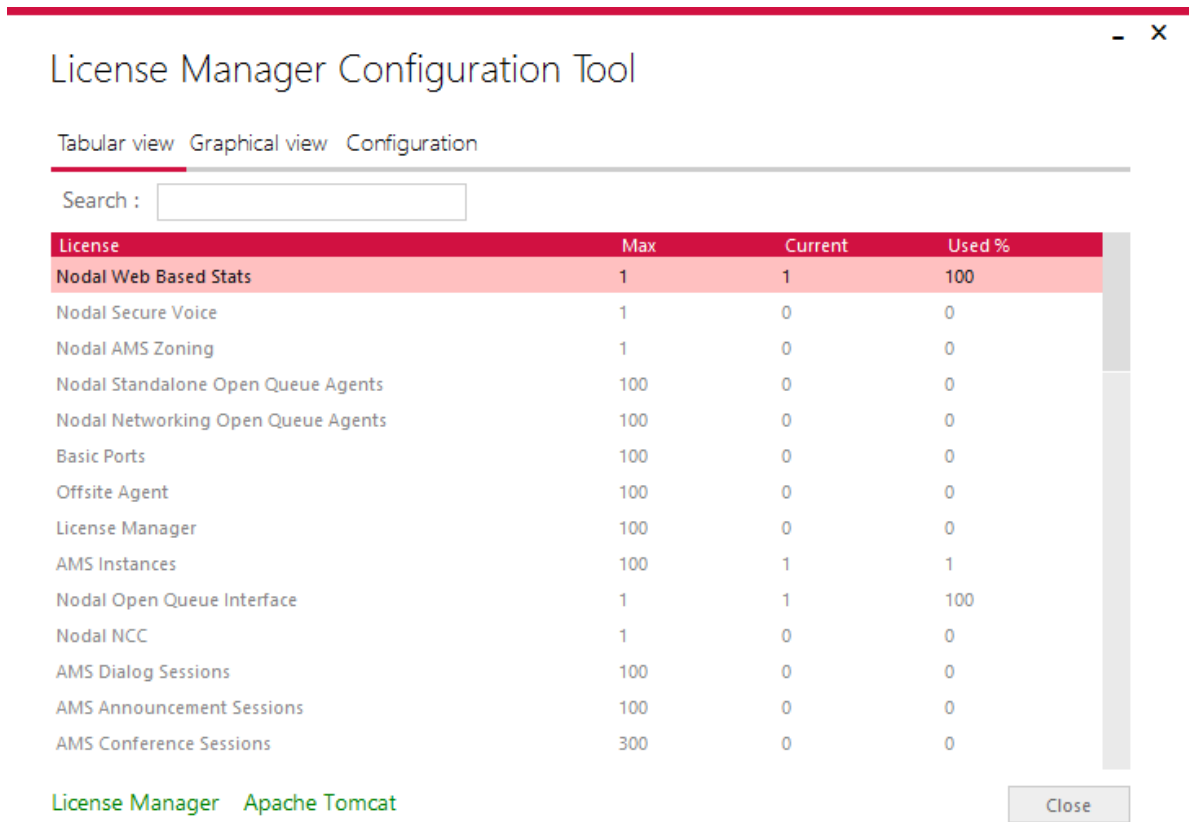
Checking the Contact Center License Manager real time usage

About this task

Check the real time usage of your contact center licenses to determine whether the necessary licenses for your Avaya Contact Center Select features are present.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the **Apps** screen, in the **Avaya** section, select **License Manager Configuration**.
3. In the Contact Center Licensing window, click **Tabular view**.



4. Ensure the license types necessary for your Avaya Contact Center Select features are present.

Using the CCMM dashboard

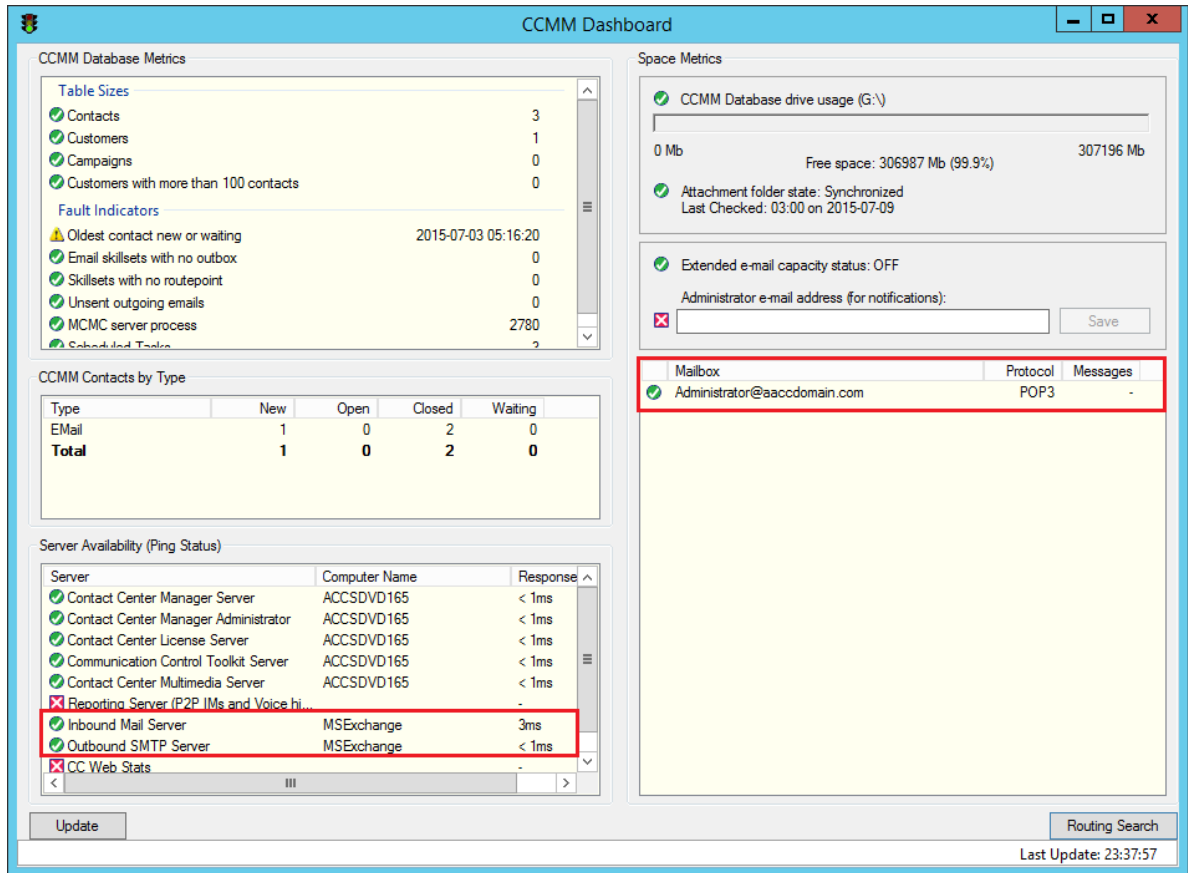
About this task

Use the CCMM dashboard to verify that Avaya Contact Center Select is communicating with the email server and is monitoring the recipient mailbox.

Procedure

1. Log on to the Avaya Contact Center Select server.
2. On the **Apps** screen, in the **Avaya** section, select **Multimedia Dashboard**.

3. Ensure Avaya Contact Center Select is communicating with the inbound email server.



4. Ensure Avaya Contact Center Select is monitoring the recipient mailbox.

Troubleshooting Contact Recording

About this task

Avaya Contact Center Select (ACCS) supports IP Office Contact Recording. IP Office uses User Rights to configure and restrict how the ACCS users access and use Contact Recording. User Rights act as templates for users, locking selected user settings to the template value. Some settings are grouped and are set and locked as a group.

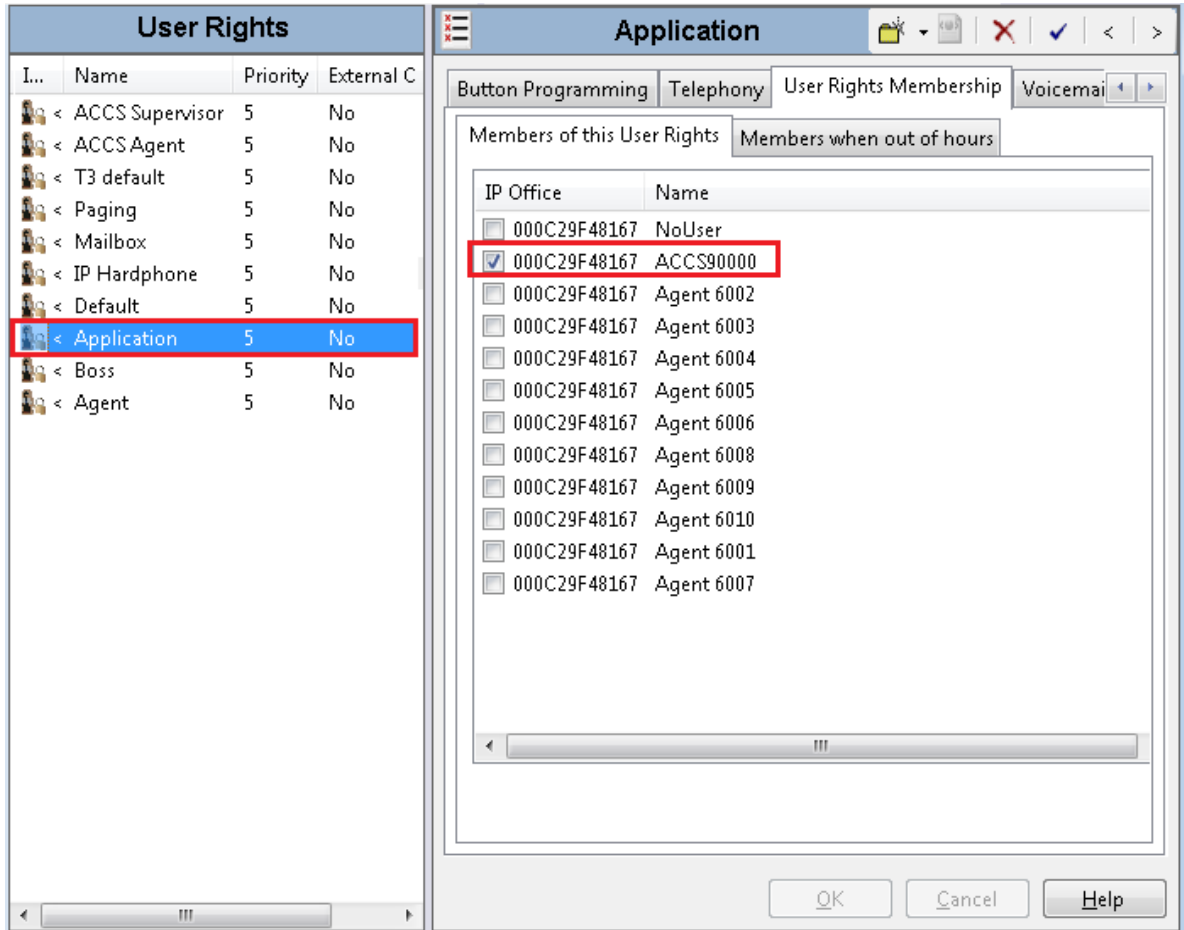
The following table shows the default IP Office User Rights for Avaya Contact Center Select (ACCS):

ACCS Resource	IP Office User Rights
ACCS SIP User Extension	Application
Agent	ACCS Agent
Supervisor agent	ACCS Supervisor

Verify that the IP Office User Rights for ACCS are configured correctly.

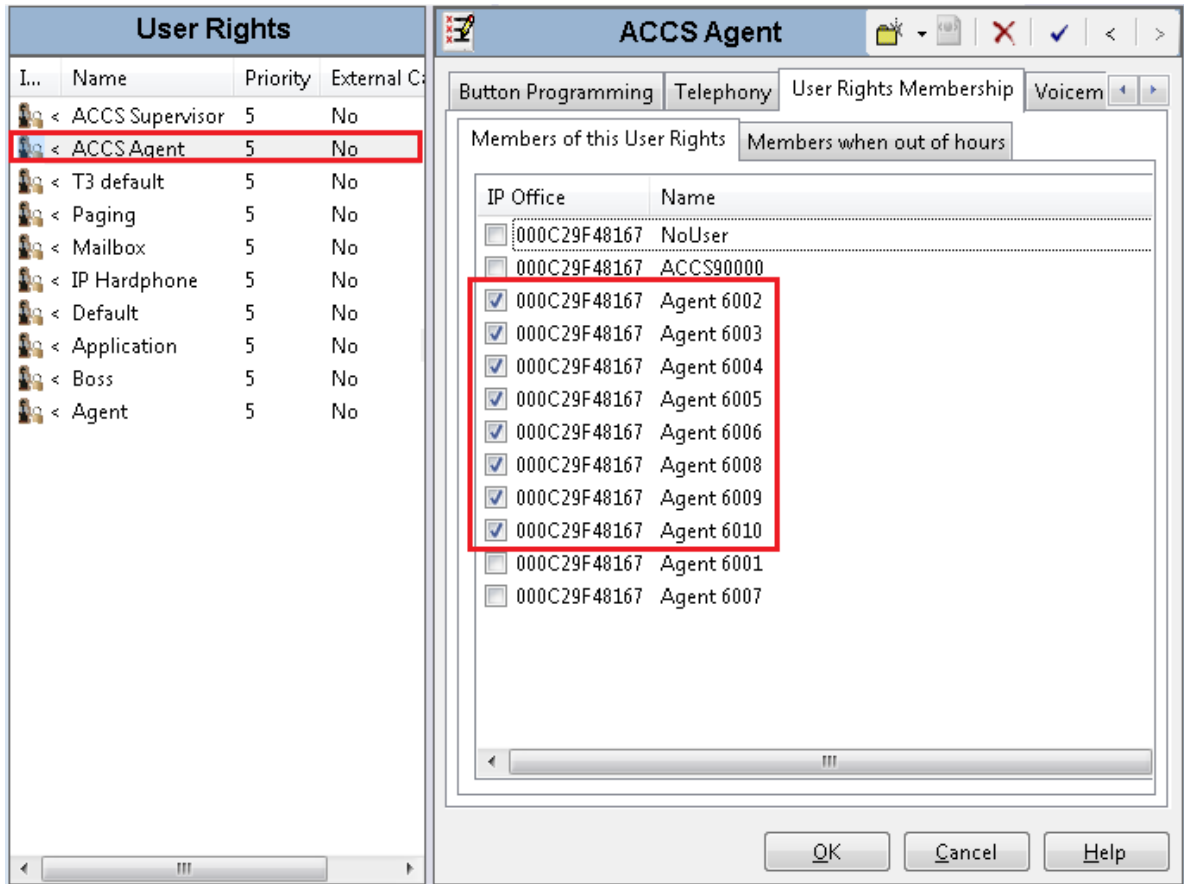
Procedure

1. Using IP Office Manager, select the IP Office server in the **Configuration** pane.
2. In the Configuration pane, under the **Solution** node, select **User Rights**.
3. In the middle pane, select **Application**.
4. Ensure the Avaya Contact Center Select SIP User Extension is assigned to the **Application — User Rights**.



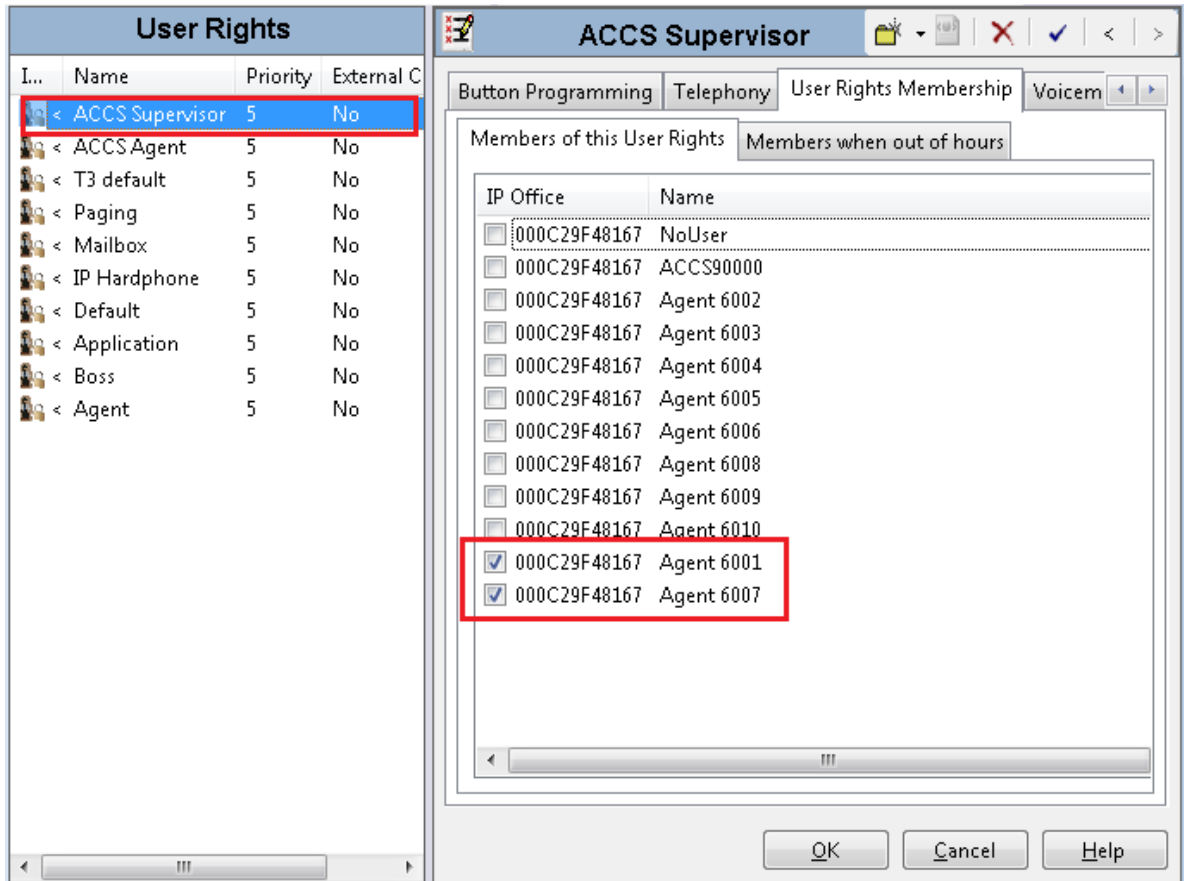
5. In the middle pane, select **ACCS Agent**.

- Ensure the Avaya Contact Center Select agents are assigned to the **ACCS Agent — User Rights**.



- In the middle pane, select **ACCS Supervisor**.

8. Ensure the Avaya Contact Center Select agents are assigned to the **ACCS Supervisor** — **User Rights**.



Chapter 22: Avaya Workspaces troubleshooting

This section describes the troubleshooting procedures that you perform when dealing with the Avaya Workspaces server.

Prerequisites for Avaya Workspaces troubleshooting

- Read the *Avaya Contact Center Select Advanced Administration* guide.
- Read the *Using Avaya Workspaces for AACC and ACCS* guide.

Logging on to the Avaya Workspaces nodes after deployment

About this task

SSH connection provides secured access to the Avaya Workspaces cluster. When logging on to any of the Avaya Workspaces nodes or master node after deployment, you must first log on as the *cust* user and then switch to the *root* user.

Use this procedure to log on to the Avaya Workspaces master node or nodes after deployment.

Procedure

1. When logging on to the Avaya Workspaces node, enter `cust` as user.
2. Enter the Avaya Workspaces cluster password.
3. Run the `su - root` command.
4. When prompted, enter the Avaya Workspaces cluster password.

Result

You are now logged on to the Avaya Workspaces node.

Troubleshooting error messages when deploying Avaya Workspaces OVA

About this task

If the host VMWare server where you deploy the Avaya Workspaces OVA is running an unsupported VMWare version, the error messages appear during the deployment process indicating that there are issues with the selected template or supported hardware versions. Use this procedure to troubleshoot this issue.

Procedure

Verify that the host VMWare server is running VMWare 6.5 or later.

Note:

The procedure of VMWare version verification differs depending on the system infrastructure. Contact your VMWare administrator to confirm the VMWare version.

Troubleshooting agent login failures

About this task

Use the following steps to troubleshoot the Avaya Workspaces authentication failures.

Procedure

1. Verify the user exists in the domain and verify the user credentials.
2. If the user is not found, verify the cluster details in the CCMM Administration tool.
3. In the CCMM Administration tool, verify that the user is synchronized in the Admin Adaptor logs.
4. In the CCMM Administration tool, verify the user details and if the domain is entered correctly.
5. Verify that the user is a domain user.

Workgroup users can not be logged in to Avaya Workspaces.

6. Debug the authentication failures by viewing the following log files:
 - cc-auth-service
 - cc-admin-adapter
 - cc-ccs-adapter

Restarting the Avaya Workspaces cluster on virtual solutions

About this task

Use this procedure to restart the Avaya Workspaces cluster on virtual solutions.

Procedure

1. Log in to your **vCenter** client.
2. Turn off the three nodes of the Avaya Workspaces cluster.
3. Turn on the **master node**.
4. Log in to the **master node** and run the `kubectl get nodes` command.
5. Verify the master node is in a `ready` state.
6. Turn on the **node1** and **node2**.
7. From the master node, run the `kubectl get nodes` command.
8. Verify all nodes are in a `ready` state.

Restarting an Avaya Workspaces container on virtual solutions

About this task

Use this procedure to restart an Avaya Workspaces container on virtual solutions.

Procedure

1. Log in to your **vCenter** client.
2. Log in to the **master node** and run the `kubectl get pods` command.
3. Verify the name of the pod you want to restart and run the `kubectl delete pod <pod name>` command.
4. From the **master node**, run the `kubectl get pods` command.
5. Verify all the pod has restarted and are in a `running` state.

Troubleshooting “helm ls” health check command

About this task

If you see the “Could not find tiller” error after entering the `helm ls` health check command, the reason is that the date/time of the node(s) does not match to the Contact Center host. Use this procedure to troubleshoot this issue.

Procedure

Re-deploy the Contact Center software.

For more information, see the Deploying documentation appropriate for your solution.

Troubleshooting “kubectl get pods --all-namespaces” health check command

About this task

If after running the `kubectl get pods --all-namespaces` command the ADF or Contact Center pods are in the state other than Running or Completed (for example, CrashLoopBackOff), this indicates a failure to start the ADF or Contact Center pods. Use this procedure to troubleshoot this issue.

Procedure

1. Navigate to `D:\Avaya\Contact Center\Workspaces\Scripts` on the Contact Center server.
2. Run the `repairworkspaces_services.bat` script on the Contact Center server.

Troubleshooting Avaya Workspaces using the Avaya Workspaces Service Utility

The Avaya Workspaces Service Utility is a standalone .NET application to perform service functions for Workspaces cluster. You can use this tool to monitor the containers and collect logs.

You can use the following tools to work with containers and logs:









Tool	Description
	Browse. Use this button to search for the config file.
	Apply. Use this button to apply the selected config file.

Table continues...

Tool	Description
	Open. Use this button to open and view the log of the selected container.
	Save. Use this button to collect logs of one or several selected containers.
	Save all. Use this button to collect all logs.
	Start. Use this button to start collecting logs.
	Stop. Use this button to stop collecting logs.
	Open folder. Use this button to open the container logs directory.
Logging interval	Select the logging interval for collecting logs.

Viewing containers

About this task

Use this procedure to view the containers on your Workspaces cluster using the Avaya Workspaces Service Utility.

Procedure

1. From the Avaya folder, click the **WorkspacesServiceUtility** shortcut to launch the Avaya Workspaces Service Utility application.

The Avaya Workspaces Service Utility application displays a list of containers stored in the default config file location.

2. (Optional) You can change the path by clicking the **Browse** button and navigating to the required location.
3. (Optional) Click the **Apply** button to display the list of containers.
4. View the containers' data:
 - Container's name
 - Node's name
 - Version
 - State

Viewing logs

About this task

Use this procedure to view the container logs using the Avaya Workspaces Service Utility.

*** Note:**

The limit for log viewing is 100 Mb. To view larger log files, use WinSCP.

Procedure

1. From the Avaya folder, click the **WorkspacesServiceUtility** shortcut to launch the Avaya Workspaces Service Utility application.

The Avaya Workspaces Service Utility application displays a list of containers.

2. To view the logs of the selected container, do one of the following:
 - Double-click a container you want to view logs of.
 - Click the **Open** button.

The logs open in the default log file editor, for example, Notepad.

3. View the logs opened.

Collecting logs

About this task

You can use the Avaya Workspaces Service Utility to collect log files. The Avaya Workspaces Service Utility provides several options for log collection:

- Collect logs of one or several containers.
- Collect all logs.
- Collect logs for a given period of time.

Use this option in a situation when you can reproduce an issue.

*** Note:**

The limit for log collection is 100 Mb. To collect larger log files, use WinSCP.

Procedure

1. Launch the Avaya Workspaces Service Utility.
2. To collect logs for one or several containers, select one or several containers and click the **Save** button.
3. To collect all logs, click the **Save all** button.
4. To collect logs for a given period of time:
 - a. Click the **Start** button.
 - b. Reproduce an issue.
 - c. Click the **Stop** button.

The Avaya Workspaces Service Utility adds the collected logs to a .zip file and displays a message once complete.

5. If you want to open the container logs directory, click the **Open folder** button.

Appendix A: VMware Best Practices

VMware Best Practices for performance

The following sections describe some of the Best Practices for VMware performance and features.

Virtualization host hardware settings

For details on BIOS settings to improve the environment for latency-sensitive workloads for an application, see the Best Practices for Performance Tuning of Latency-Sensitive Workloads in vSphere VMs technical white paper at <http://www.vmware.com>.

The following are the best performance BIOS settings for a few specific servers from the VMware-certified server list. In general, turn off power-saving server options for optimal performance. Consult the manufacturer technical data for your particular server.

Intel Virtualization Technology support

Intel CPUs require EM64T and Virtualization Technology (VT) support in the chip and in the BIOS to run 64-bit virtual machines.

All Intel Xeon processors feature:

- Intel Virtualization Technology
- Intel Extended Memory 64 Technology
- Execute Disable Bit

Ensure that VT is enabled in the host system BIOS. The feature might be called VT, Vanderpool Technology, Virtualization Technology, VMX, or Virtual Machine Extensions.

*** Note:**

The VT setting is locked (either on or off) at boot time. After enabling VT in the system BIOS, save your changes to the BIOS settings and exit. The host server reboots, and the BIOS changes take effect.

Other virtualization host hardware settings

Servers with Intel Nehalem class and newer Intel Xeon CPUs also offer two power management options: C-states and Intel Turbo Boost.

- Disabling C-states lowers latencies to activate the CPUs from halt or idle states to full power on.

- Intel Turbo Boost steps up the internal frequency of the processor if the workload requires more power. The default for this option is enabled. Do not change the default.

These settings depend on the OEM make and model of the server. The BIOS parameter terminology for current Dell and HP servers are described in the following sections. Other server make and models can have other terminology but equivalent BIOS controls.

Dell PowerEdge Servers — Hardware settings

When the Dell server starts, you select F2 to display the system setup options. The following are the recommended BIOS settings for the Dell PowerEdge servers:

- Set the Power Management Mode to **Maximum Performance**.
- Set the CPU Power and Performance Management Mode to **Maximum Performance**.
- Under Processor Settings, set **Turbo Mode** to **enable**.
- Under Processor Settings, set **C States** to **disabled**.

HP ProLiant Servers — Hardware settings

The following are the recommended BIOS settings for the HP ProLiant servers:

- Set the Power Regulator Mode to **Static High Mode**.
- Disable **Processor C-State Support**.
- Disable **Processor C1E Support**.
- Disable **QPI Power Management**.
- Enable **Intel Turbo Boost**.

VMware networking best practices

There are many different ways of configuring networking in a VMware environment. Review the VMware networking best practices documentation before deploying Avaya applications on an ESXi host. This section is not a substitute for the VMware documentation. For improved performance and best practice, Contact Center uses Network Adapter type VMXNET 3.

The following are some suggested networking best practices:

- Separate network services to achieve greater security and performance. Create a vSphere *Standard Switch* with dedicated NICs for each service. Separate VMware Management, iSCSI (SAN traffic), and VM networks to separate physical NICs. If separate switches are not possible, consider port groups with different VLAN IDs.
- All physical NICs that are connected to the same vSphere *Standard Switch* must be connected to the same physical network.
- Configure all VMkernel vNICs to the same MTU (IP Maximum Transmission Unit).
- Configure Contact Center to use Network Adapter type VMXNET 3.

For more information about VMware networking best practices, refer to the VMware documentation.

VMware Tools

VMware Tools are included as part of the application OVA. The tools are a suite of utilities that enhances the performance of the operating system on the virtual machine and improves the management of the virtual machine.

The tools provide:

- VMware Network acceleration
- Host to virtual machine time synchronization
- Disk sizing
- Startup/Shutdown

 **Note:**

Do not upgrade the VMware tools software which is packaged with each OVA unless instructed to do so by Avaya.

Network Time Protocol and time configuration

For accurate time keeping, use the Network Time Protocol (NTP) as a time source instead of the ESXi hypervisor.

The NTP servers can be local to the LAN or over the Internet. If the NTP servers are on the Internet, the corporate firewall must open UDP port 123 so that NTP service can communicate with the external NTP servers.

Troubleshooting VMware

Virtualization platform performance issues can result with Contact Center performance problems. The virtualization platform includes the host and the running virtual machines on the host. Contact Center performance problems can include but are not limited to high CPU usage, link instability, defaulted or abandoned calls.

You must logically and systematically investigate any Contact Center performance issues to rule out virtualization performance problems. All deviations from the published specifications must be investigated and resolved before the Contact Center software investigation is initiated. For more information, refer to the VMware vSphere documentation.

To support troubleshooting VMware resourcing issues, collect information about the following VMware Key Performance Indicators (KPIs).

VMware vSphere Host KPIs:

- Physical CPU
 - PCPU - Physical CPU usage.
 - CPU load average - Average CPU load average of host.
- Physical Memory
 - SWAP/MB - Memory swap usage statistics.

VMware vSphere Virtual Machine (VM) KPIs:

- vCPU
 - CPU RDY - Time VM was ready to run, but was not provided CPU resource.
 - CPU WAIT - Percentage of time spent in the blocked or busy wait state.
 - AMIN - Reservation allocated.
 - ASHRS - CPU shares allocated.
 - CPU CSTP - Amount of time a Symmetric Multi-Processing (SMP) VM was ready to run, but was delayed due to co-vCPU scheduling contention.
- Disk I/O
 - GAVG - Average operating system read latency per read operation.
 - DAVG/rd - Average device read latency per read operation.
 - DAVG/wr - Average device write latency per write operation.
 - RESETS/s - Number of commands reset per second.
 - ABRTS/s - Number of disk commands abandoned per second.
- Network
 - %DRPTX - Percentage of packets dropped when transmitting.
 - %DRPRX - Percentage of packets dropped when receiving.
- Memory
 - MCTLSZ - Amount of physical memory reclaimed memory balloon statistics.

Index

A

activity code	
enter	206
add	
server to domain	214
adding agents	256
administration	
users	255
agent adding	256
agent changing	259
agent copying	260
Agent Desktop	194 , 263
action bar	197
install	199 , 263
log off	211
top bar	195
user interface	194
agent login failures	296
applications check variable references	248
auto restart delay	170
Automatic Maintenance	129 , 144 , 222 , 223
automatic startup settings	152
Avaya Aura Media Server	77
patching	226
Avaya Aura Media Server installing patches	101
Avaya Aura Media Server OVA	80 , 84 , 89 , 92
Avaya IX Workspaces	295
Avaya support website	15
Avaya WebLM OVA	52
Avaya Workspaces	155 , 158 , 161 , 174 , 298
Avaya Workspaces deployment	296
Avaya Workspaces OVA	156
Avaya Workspaces Service Utility	299 , 300

B

backing up	215
backup location	217
Best Practices	302
BIOS	302
BIOS settings	303

C

call	
accepting	205
end	206
make	207
CCMA logging on	256
CCMA starting Variables tool	247
changing agent	259
changing variable properties	248 , 250 , 251

checking variable references	248
checklist	26–28
collecting logs	300
compatibility list view	245
configuration	158
configuration details	
AAMS OVA	97
WebLM OVA	72
configure	
Session Border Controller	181
configuring	174
Session Border Controller networks	181
Configuring a TLS client profile on Avaya Aura Session	
Border controller	190
Configuring a TLS server profile	189
configuring Internet Explorer for CCMA	232
Configuring Internet Explorer integration	235
connection	
contact center subnet	125
connectivity details	180
Contact Center	215 , 222
contact recording	164 , 291
Contact Recording	44
copying agent properties	260
CPU Cores	98 , 151
creating	
client profile	184
reverse proxy policy	182
reverse proxy service	191
server profile	185
creating variables in CCMA	247

D

dashboard	145 , 275 , 290
data synchronization	35
deployment	161
deployment process	25 , 155
details for agents changes	259
disable	
unused Network Adapters	126
disable Admin Approval Mode	
Windows Server administrators	127
disabling	
IE mode	246
disk partitions	115 , 122
documentation	220
download	
recent server patches	126
downloading latest patches	221
DVD installation	129

E

Element Manager	99
email	198
accept	208
email message	209
enable	
Microsoft Remote Desktop connection	127
Enterprise Mode Site List	236
extensions	48
external firewall	178

G

gateway	38
---------------	--------------------

H

hard disk partitions	115 , 122
health check	298
health check troubleshooting	298

I

IE mode	
configure compatibility list view	245
configure on local computer	244
creating configuration file	240
disable	246
enabling on domain server	243
installing administrative templates	239
IE Mode	234–236 , 238
immediate backups	215
install	
Agent Desktop	199 , 263
installing Avaya Aura Media Server patches	101
installing Avaya Aura Media Server patches on linux	226
Intel	302
Internet Explorer	235 , 236
Internet Explorer mode	234 , 238
IP Office	33
IP Office Manager	34 , 49 , 164 , 172
IP Office service user	37
IP Office support	33
IP Route	38
IP User Extension Number	286

L

latest documentation	220
license	289
logging on	256
logging on to Agent Desktop	200
logging on to CCMA	256

M

maintenance	214
management adding agent	256
Microsoft Edge	234–236 , 238
Microsoft Edge administrative templates	234
Microsoft Windows Server 2012 R2	116
Microsoft Windows Server 2016	123
Microsoft Windows Server 2019	123
misconfiguration	272

N

NTP	304
-----------	---------------------

O

operating system	124 , 220
operating system service packs	124 , 220
OVA	225
overview	22

P

patches	221 , 222
pause recording button	166
phone set configuration	180
prerequisites	176
properties changing for variables	248 , 250 , 251
properties of agents copying	260
Purpose	12

R

Ready status	204
real time reports	268
real-time display	268
recent patches downloads	221
related documentation	12
release notes	220
remote access	
configuration	174
configuring	174
Remote proxy	189
remote worker	180
restarting Avaya Workspaces cluster	297
restarting Avaya Workspaces container	297
reverse proxy	174 , 176 , 179 , 187
Reverse proxy	174 , 175 , 190
reverse proxy configuration process flow	176

S

scheduled backup	217
scheduled backup location	217
scheduling backup	

Index

scheduling backup (<i>continued</i>)		VMware virtual machine	106
Contact Center Server	218	VMXNET	303
script variables in CCMA	247	voice prompt	253
server preparation	124, 220	vSphere	55, 64, 80, 89, 92
adding a server to a domain	214		
disabling unused Network Adapters	126	W	
download recent patches to the server	126	WebLM	52
downloading latest documentation	106	WebLM license file	75
enable Microsoft Remote Desktop connection	127	WebLM OVA	55, 60, 64, 68
server services	227	WebLM server Host ID	73
service packs	124, 220	Windows Server	
shared location		disable UAC	127
CSR export	128	Windows Server 2016 UI	123
short code	42	Windows Server 2019 UI	123
silent install	264, 265	Windows services	227
SIP domain	40	work item paradigm	195
SIP user extension number	42	work list window	196
software appliance	12	Workspaces Service Utility	298
software installation			
disable Admin Approval Mode	127		
solution architecture overview	175		
SSH login	295		
support	15		
Supported contact types	174		
T			
test email	207		
test phone call	204		
troubleshooting	272, 298		
troubleshooting Avaya Workspaces	295		
troubleshooting symptoms	273		
types of variables changing	248, 250, 251		
U			
unsecure CTI for IP Office	150		
users			
administration	255		
V			
variables changing properties	248, 250, 251		
variables checking for references	248		
variables in CCMA	247		
vCenter	60, 68, 84		
verifying patches are up-to-date	221		
videos	14		
viewing containers	299		
viewing logs	299		
virtual deployment	156		
virtual machine	104, 115, 122		
virtual solution	297		
virtual solutions	297		
Virtualization	304		
VMware Tools	125, 304		