Deploying Avaya Workspaces for Elite

Release 3.6.1
Issue 1.2
July 2019

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. 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.

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are

not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction 9
- Purpose 9
- Change history 9
- Prerequisites 9
- Changes in this release 9
  - Avaya Proactive Outreach Manager enhancements 10
  - Support for automated migration process 10

Chapter 2: Overview 11
- Avaya Workspaces for Elite overview 11
- Topology 12

Chapter 3: Deployment process 14
- Deployment process flow 14

Chapter 4: Planning and preconfiguration 15
- Planning and preconfiguration 15
  - Hardware requirements 15
  - Client specifications 16
  - Capacity specifications 17
  - Minimum supported browser versions 18
  - Licensing 19
  - Virtual Machine requirements 19
  - VMware configuration 21
  - Configuration and deployment details 21

Chapter 5: Deploy Avaya Breeze® platform nodes 24
- Deploy Avaya Breeze® platform nodes 24
  - Avaya Breeze® platform nodes deployment checklist 25
  - Verifying the Avaya Breeze® platform deployment using System Manager 26
  - Configuring LDAP server certificates for Avaya Breeze® platform nodes 27
  - Configuring LDAP server integration 28
  - Avaya Workspaces single sign-on 30
  - Configuring the WebSphere certificate for Centralized Logging 31
  - Creating the common certificate 31
  - Importing the common certificate in Avaya Breeze® platform nodes 32
  - Exporting the Avaya Breeze® platform Authorization Identity Certificate 33

Chapter 6: Configure Application Enablement Services 34
- Configure Application Enablement Services 34
  - Configuring Communication Manager Link to Application Enablement Services 34
  - Configuring AES certificates 36
  - Creating Application Enablement Services user for Call Server Connector communication 38
  - Verifying Application Enablement Services connection with Call Server Connector service 39

Chapter 7: Configure Communication Manager resources 40
Configure Communication Manager resources for Avaya Workspaces for Elite 40
Logging on to Communication Manager 41
Configuring System Features and Customer Options 42
Configuring Signaling and Trunk Groups 43
Configuring a Route Pattern 43
Adding a Route Pattern to the Locations table 44
Configuring CTI-Link to Application Enablement Services 44
Configuring Direct Agent Calling 45
Configuring a Hunt Group for Avaya Workspaces for Elite 46
Creating variables using Communication Manager 48
Configuring VDN's and vectors for Avaya Workspaces for Elite 50
Configuring Agent Login ID using Communication Manager 53
Configuring Agent Phone-sets 54
Adding AUX codes 54
Configuring auto answer 57
Configuring auto-in and manual-in station buttons 58
Chapter 8: Deploy clusters 60
Deploy Avaya Workspaces for Elite clusters 60
Verifying host name resolution for Avaya Breeze® platform nodes 61
Loading license files in System Manager 62
Loading SVARs in System Manager 62
Creating Avaya Workspaces for Elite Cluster 1 64
Creating Avaya Workspaces for Elite Cluster 2 66
Setting cluster services attributes 67
Adding nodes to Avaya Workspaces for Elite cluster 1 71
Adding nodes to Avaya Workspaces for Elite cluster 2 72
Verifying the status of Avaya Breeze® platform nodes 73
Setting Cluster State to Accepting 73
Enabling CORS for clusters 74
Certificate-based authentication 74
Verifying Application Enablement Services connection with Call Server Connector service 75
Installing the Authorization Identity Certificate on the cluster 75
Viewing Oceana Monitor Service pages 76
Rebooting the Avaya Workspaces for Elite cluster 77
Chapter 9: Commission Avaya Workspaces for Elite 79
Commission Avaya Workspaces for Elite 79
Creating a Communication Manager user for Avaya Control Manager 79
Logging in to Avaya Control Manager 80
Creating a location for Avaya Workspaces for Elite 81
Adding Communication Manager to Avaya Control Manager 81
Adding Communication Manager to the Avaya Workspaces for Elite location 82
Assigning the Avaya Workspaces for Elite location to UCA Proxy Server 83

Assigning the Avaya Workspaces for Elite location to Application Server 83
Assigning the Avaya Workspaces for Elite location to Synchronizer Service Server 84
Adding site, department, and team to Avaya Control Manager 85
Synchronizing Avaya Control Manager and Communication Manager 86
Creating an Avaya Workspaces for Elite server 87
Adding the Avaya Workspaces for Elite server to the Avaya Workspaces for Elite location 87
Configuring the Avaya Workspaces for Elite server 88
Configuring AUX codes 89
Adding connectors to the Provisioning Server 90
Testing the UCA REST connection 91
Configuring a secure connection between Avaya Control Manager and the Avaya Workspaces for Elite server 92
Creating an Avaya Workspaces agent user to handle Elite Voice contacts 97
Creating an Avaya Workspaces supervisor user 98
Creating an Avaya Workspaces administrator user 100
Configuring screenpops 101
Configuring CRM integration 103
Enabling Avaya Breeze® platform authorization on Avaya Aura® Device Services 104
Configuring LDAP integration 104
Support for handling browser close and network connection issues 105
Chapter 10: Post-installation verification 107
Verifying the Avaya Workspaces installation 107
Chapter 11: Administration 108
Avaya Workspaces for Elite administration 108
Enabling After Contact Work 108
Using the Avaya Workspaces compressed layout 109
Configuring start work button behavior 109
User tokens 109
Chapter 12: Upgrade Avaya Workspaces for Elite 111
Preupgrade tasks 111
Adding a third-party root certificate to a cluster 111
Replacing node identity certificates by a third-party certificate 111
Upgrade System Manager and Avaya Control Manager 112
Automated upgrade 112
Automated upgrade overview 112
Automated upgrade checklist 113
Checking the stability of Avaya Breeze® platform nodes 114
Checking the replication status of Avaya Breeze® platform nodes 114
Checking the state of services 114
Upgrading Avaya Breeze® platform 115
Refreshing the Authorization Service identity certificates 117
Manual upgrade 117
Manual upgrade overview 117

Manual upgrade checklist 118
Setting Cluster State to Denying 119
Uninstalling all services from the clusters 119
Deleting all services from System Manager 120
Upgrading Avaya Breeze® platform nodes using the ISO file 120
Applying the Avaya Breeze® platform patch 121
Installing services to the clusters 121
Setting Cluster State to Accepting 122
Chapter 13: Centralized Logging 124
Centralized Logging 124
Configuring Avaya Workspaces for Elite Cluster 2 for Centralized Logging 124
Security configuration for Centralized Logging 125
Logging in to Kibana 125
Creating an index pattern in Kibana 125
Searching logs in Kibana 126
Viewing statistics on the Metricbeat dashboard 127
Viewing statistics on the Packetbeat dashboard 127
Chapter 14: Logging 128
Logs 128
Downloading the Avaya Workspaces logs 128
Modifying the logging configuration 129
Chapter 15: Troubleshooting 130
Internet Explorer 11 does not display the fonts correctly 130
Chapter 16: Resources 131
Documentation 131
Finding documents on the Avaya Support website 131
Avaya Documentation Portal navigation 132
Training 133
Support 133
Using the Avaya InSite Knowledge Base 133

Chapter 1: Introduction

Purpose

This document describes installation, configuration, and administration procedures for Avaya Workspaces for Elite.

Administrators can use this document to install and configure a verified Avaya Workspaces for Elite reference configuration at a customer site.

Change history

Issue	Date	Summary of changes
1.2	July 25, 2019	Minor updates to Planning and preconfiguration on page 15.
1.1	July 24, 2019	Minor updates to the Upgrade chapter.

Prerequisites

Before deploying Avaya Workspaces, ensure that you have a working knowledge of the following products:

- Avaya Breeze® platform
- Avaya Aura® Communication Manager
- Avaya Aura® System Manager
- Avaya Control Manager

Changes in this release

Avaya Workspaces for Elite Release 3.6.1 includes the following changes:

Avaya Proactive Outreach Manager enhancements

Avaya Workspaces for Elite provides the functionality to handle Outbound contacts. With this functionality, agents sign in to Avaya Proactive Outreach Manager (POM) and Avaya Workspaces for Elite, and work with the Outbound contacts that they receive.

In this release, the Widget API Framework is extended to enhance POM interactions in Avaya Workspaces for Elite.

Support for automated migration process

The current release of Avaya Workspaces for Elite supports automated migration process. You can run the automated script to upgrade Avaya Breeze® platform nodes and the services of Avaya Workspaces for Elite clusters.

Chapter 2: Overview

Avaya Workspaces for Elite overview

Avaya Workspaces for Elite is a browser-based application with which Contact Center agents can handle customer interactions. Avaya Workspaces for Elite supports the voice channel only. Agents can also make outbound voice calls. The intuitive user interface provides features for toggling between multiple interactions.

Note:

This document does not describe how to deploy a Call Center Elite solution; this document assumes that Call Center Elite is already deployed and is operational.

The application enables seamless collaboration with customers, partners, and other users within and outside the organization. It also provides relevant information to agents securely and reliably.

Every interaction is displayed as an interaction card. Using interaction cards, agents can:

- Receive the interaction: Accept interactions with a single click.
- Hold or resume the interaction: Put an active voice interaction on hold when another interaction with a higher priority must be attended to.
- Consult another agent: Seek advice about an interaction.
- Transfer the interaction to another agent: Send the interaction to another agent interaction area.
- Add another agent to the interaction: Create a conference with another agent when the other agent can contribute to resolving the customer interaction.

To enhance accessibility, Avaya Workspaces provides:

- Access to most content and controls by using the keyboard.
- Alternative text and labels to assist users with screen readers.
- Screen magnifier tool, such as Magnifier, to zoom in and out of Avaya Workspaces screens.

  Do not use built-in controls of the browser.

Features

Avaya Workspaces for Elite provides the following features:

- Screenpops: Agents are presented with external webpages that can assist them in completing their tasks. For example, external websites with information such as current currency exchange rates.

- Customer journey: The system displays a graphical representation of the customer interactions. Every point in the customer journey is visualized by an interaction. This feature is an optional add-on, and requires custom integration.

Limitations

The following limitations apply to the Avaya Workspaces for Elite solution:

- Avaya Workspaces for Elite supports the voice channel only. Digital channels are not supported.
- The pool of agent stations for Avaya Workspaces for Elite must be for use only by Avaya Workspaces for Elite users.
- Auto answer is supported, however there are limitations that you must consider. See Configure Communication Manager resources for Avaya Workspaces for Elite on page 40.

Topology

The following diagram depicts the architecture for the deployment of a typical Avaya Workspaces for Elite solution with a maximum capacity of 1000 agents.

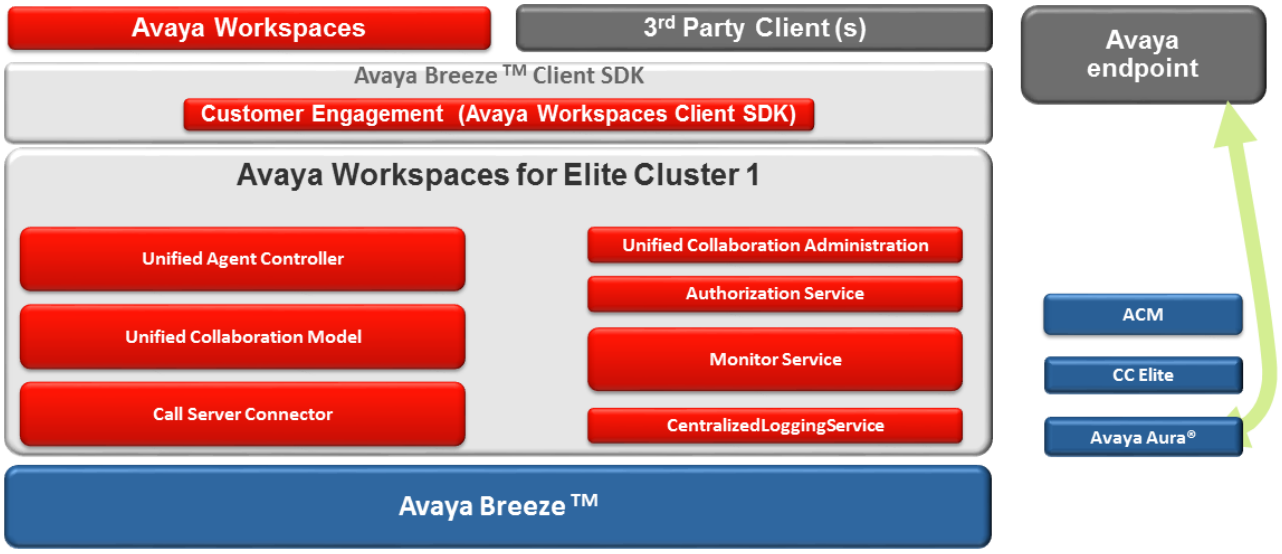


Figure 1: Topology - small solution

The following diagram depicts the architecture for the deployment of a typical Avaya Workspaces for Elite solution with a maximum capacity of 7500 agents.

Figure 2: Topology - large solution

Chapter 3: Deployment process

Deployment process flow

This task flow shows you the sequence of procedures you must perform to deploy an Avaya Workspaces for Elite solution:

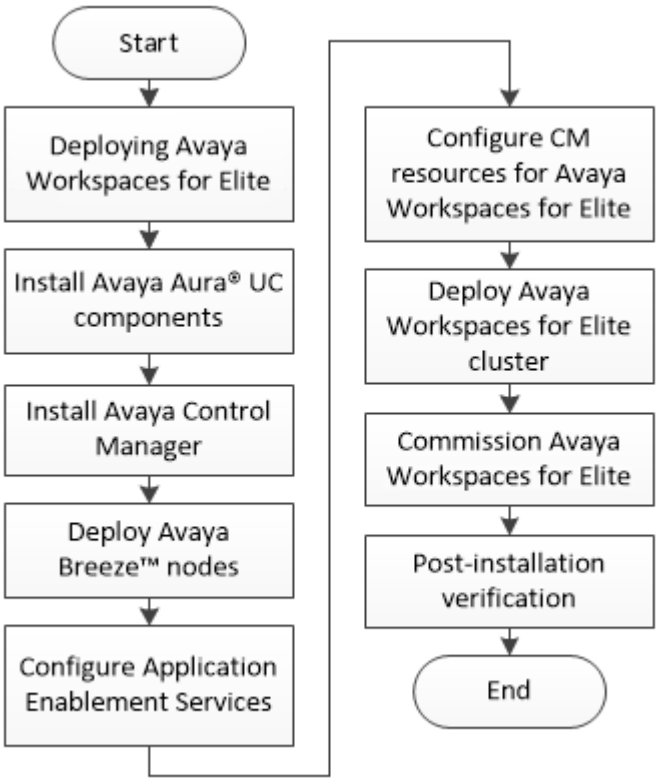


Figure 3: Deployment process

Chapter 4: Planning and preconfiguration

Planning and preconfiguration

This section specifies the interoperability requirements to deploy Avaya Workspaces for Elite.

You must install and commission the following Avaya Aura® Unified Communications components to support voice routing for the Avaya Workspaces for Elite solution. This document assumes that these components are already installed and configured:

Component	Supported release
Avaya Aura® System Manager	8.0.x and 8.1
Avaya Aura® Communication Manager	7.x, 8.0.x, and 8.1
Avaya Aura® Call Center Elite	7.x, 8.0.x, and 8.1
Avaya Aura® Session Manager	7.x, 8.0.x, and 8.1
Avaya Aura® Application Enablement Services	7.x, 8.0.x, and 8.1

Note:

Elite pending states are supported only with Avaya Aura® Unified Communications 7.1.2 or later, and you must set the AES ASAI Link Version to 8 or later.

You must also install and commission the following version of Avaya Control Manager to support administration for the Avaya Workspaces for Elite solution. This document assumes that Avaya Control Manager is already installed and configured:

Component	Supported release
Avaya Control Manager	8.1.0.1

For the most recent information, see the individual product Release Notes available on https://support.avaya.com.

- Ensure that all your server hardware and virtualization infrastructure meet the requirements.
- Ensure that you have sufficient knowledge about the installation and configuration that you want to use in your solution.

Hardware requirements

The following table provides information about the memory, disk, and vCPU requirements for the components required to support Avaya Workspaces for Elite:

Component	Platform	Requirement	Avaya Workspaces for Elite	
			7500 agent maximum	1000 agent maximum
Avaya Workspaces for Elite cluster 1	Avaya Breeze® platform	Number of nodes	3	3
		Memory/node	32 GB	24 GB
		Minimum disk size/node	500 GB	500 GB
		vCPU's/node	8	6
Avaya Workspaces for Elite cluster 2	Avaya Breeze® platform	Number of nodes	2	n/a
		Memory/node	32 GB	n/a
		Minimum disk size/node	500 GB	n/a
		vCPU's/node	12	n/a
Avaya Control Manager	Windows	Number of nodes	1	1
		Memory/node	12 GB	12 GB
		Minimum disk size/node	300 GB	300 GB
		vCPU's/node	8	8
Avaya Control Manager database server	Windows	Number of nodes	1	1
		Memory/node	12 GB	12 GB
		Minimum disk size/node	300 GB	300 GB
		vCPU's/node	8	8

Note:

- Each Avaya Breeze® platform node of a cluster must reside on a different virtual server.
- The current release of Avaya Workspaces for Elite supports VMware ESXi 6.0, 6.5, and 6.7.
- Avaya recommends using 15000 RPM disks. Avaya Oceana® Solution does not support Solid State Drives (SSD).

Client specifications

To use Avaya Workspaces, your client computer must meet the following requirements:

Hardware specifications

- 3.20 GHz or higher Intel Core processor
- 8 GB of RAM
- 300 GB available hard disk space

- Intel HD Integrated Graphics
- Super VGA monitor (15 inches or larger)
- Minimum screen resolution of 1024 x 768

Supported operating systems

- Microsoft Windows 10 (x32 and x64)
- Apple Mac OS 10.11

Latency

Avaya Workspaces performance can degrade or become unresponsive if you use a network connection with a latency of more than 300 milliseconds Round Trip Time (RTT).

Capacity specifications

The following table shows the capacity specifications for an Avaya Workspaces for Elite deployment:

Parameter	Maximum for large solution	Maximum for small solution
Maximum number of active Avaya Workspaces Agents	7500	1000
Maximum number of configured Agents	22500	3000
Maximum number of configured Supervisors	2250	300
Maximum number of configured users (Agents and Supervisors)	24750 (22500 and 2250)	3300 (3000 and 300)
Maximum number of concurrent Avaya Workspaces instances per Agent	1	1
Maximum number of concurrent Avaya Workspaces instances per Supervisor	1	1
Maximum supported Voice Busy Hour Call Completion (BHCC) - Self Service	This figure depends on your Avaya Aura® solution. For more information, see *Avaya Aura® Communication Manager System Capacities Table*.	This figure depends on your Avaya Aura® solution. For more information, see *Avaya Aura® Communication Manager System Capacities Table*.
Maximum supported Voice Busy Hour Call Completion (BHCC) - Assisted Service	This figure depends on your Avaya Aura® solution. For more information, see *Avaya Aura® Communication Manager System Capacities Table*.	This figure depends on your Avaya Aura® solution. For more information, see *Avaya Aura® Communication Manager System Capacities Table*.

Table continues…

Parameter	Maximum for large solution	Maximum for small solution
Maximum queued Voice contacts	This figure depends on your Avaya Aura® solution. For more information, see *Avaya Aura® Communication Manager System Capacities Table*.	This figure depends on your Avaya Aura® solution. For more information, see *Avaya Aura® Communication Manager System Capacities Table*.
Maximum number of Communication Managers	• 1 CM/CCElite Simplex • 1 CM/CCElite Duplex • 1 CM/CCElite Simplex or Duplex with associated ESS	• 1 CM/CCElite Simplex • 1 CM/CCElite Duplex • 1 CM/CCElite Simplex or Duplex with associated ESS

Minimum supported browser versions

- Google Chrome 62 to 71
- Microsoft Internet Explorer 11
- Apple Safari 11, 12
- Microsoft Edge 41 to 44

Browser limitations

Internet Explorer 11 limitations

The following are the inherent limitations of the browser.

- Internet Explorer 11 does not support plug-ins and extensions.
- Internet Explorer 11 cannot handle multiple workcards.
- Internet Explorer 11 browser leaks memory. The browser becomes unresponsive after a period of time. The length of time depends on your hardware and the extent of agent activity.
- Internet Explorer 11 can cause other websites to freeze and can impact Avaya Workspaces operation.
- Widgets with a large amount of data affect the performance of Internet Explorer 11.
- On Internet Explorer 11, when using Supervisor Dashboard, the scroll bar scrolls the entire widget. For filtering and searching, if you have already scrolled down, you need to scroll up to the search area.
- When you complete an interaction, Internet Explorer 11 does not close the opened screenpop and does not display the buttons to view and close the screenpop.

Recommendations:

- You must log out and restart the Internet Explorer 11 browser regularly.

- You must manually click to view the Avaya Workspaces Welcome and Screen-pop widgets. These widgets load third-party websites that the administrator configures.
- You must manually activate the Customer Journey widget as it uses charts to visualize the data.
- You must not have multiple Internet Explorer 11 tabs open at the same time as Avaya Workspaces.
- If you select the **Enable protected mode** option on Internet Explorer 11 security settings, the browser does not have a reference to opened screenpops.

Apple Safari 11 limitations

The following limitations are due to compatibility issues with Apple Safari 11.

- If you refresh the browser window during an active session in Avaya Workspaces, the browser window goes blank.
- Apple Safari 11 does not support downloading logs from Avaya Workspaces.

Recommendation:

When Apple Safari 11 goes blank, open **Developer tools** on the browser, clear local settings, and close all browser instances before reloading Avaya Workspaces.

Licensing

In addition to Avaya Aura® Call Center Elite licenses, each user also requires a Avaya Workspaces for Elite license. You must ensure that you have the required number of licenses to support the planned maximum number of agents that use Avaya Workspaces for Elite simultaneously.

The base license includes licenses for all of the components required in an Avaya Workspaces for Elite solution, for example Avaya Breeze® platform, Avaya Control Manager, and Avaya Aura® Communication Manager.

Virtual Machine requirements

ESXi hosts specification

The following table lists the minimum specifications required for ESXi hosts that you install Avaya Breeze® platform nodes on:

Processor	Intel Xeon E5-2697 2.60GHz
Network Interface	Network Interface Controller (NIC)
Disk type and speed	SATA, Minimum 15000 RPM

Virtual resource allocation in vSphere

RAM

On a Virtual Machine, the following two values are associated with RAM:

- Allocated RAM (ARAM)
- Reserved RAM (RRAM)

If RRAM is less than ARAM, VMware creates a file of size ARAM - RRAM, and uses the file as RAM if there is contention for RAM resources. The performance is impacted as you switch from RAM I/O to file I/O. Therefore, you must always reserve ARAM.

CPU

- Ensure that Hyperthreading is turned on.
- Ensure that CPU meets or exceeds the benchmark rating for Intel Xeon E5-2697 (first edition) 2.60GHz.

  You can find a sample benchmark on https://www.cpubenchmark.net.
- Refer to VMware documentation for information about interpreting esxtop statistics, to allow you to investigate and avoid performance problems at the virtualization layer.
- Observe the following counters for using esxtop data at the host level:
  - CPU Load Average: A load average of 1.00 indicates that the physical CPUs of the host are fully utilized. A load average of 0.5 indicates that the physical CPUs of the host are half utilized. Any value greater than 1 indicates performance problems.

    Note:

    Performance problems can also occur with values less than 1.
  - Physical CPU: Ensure that the Physical CPU usage does not exceed 80%. Performance is impacted if the Physical CPU usage consistently exceeds 80%.
- Observe the following for using esxtop data at the Virtual Machine level:
  - RDY: The percentage of time that something is waiting for a CPU to be available to execute its workload. Ensure that RDY does not exceed 5% for any vCPU.
  - MLMTD: The percentage of time that a vCPU was waiting due to a limit set on the Virtual Machine for CPU usage. Ensure that you increase or remove your limit if this value is greater than 0.

A lot of data is available through esxtop and VMware Infrastructure Client for all levels of granularity, from host through Virtual Machine and per vCPU.

VMware configuration

VMware feature	Supported on Avaya Workspaces for Elite clusters on VM with live traffic in production	Supported on Avaya Workspaces for Elite clusters in maintenance mode*
Cloning	No	Yes
Distributed Power management (DPM)	No	No
Distributed Resource Scheduler (DRS)	No	No
Distributed Switch	No	No
Fault Tolerance	No	No
High Availability (HA)	No	No
Snapshot	No	Yes**
Storage DRS	No	No
Storage Thin Provisioning	No	No
Storage vMotion	No	Yes
Suspend & Resume	No	NA
vMotion	No	Yes

* Maintenance mode specifies a scheduled out-of-production window where the system does not process contacts, agents are all logged out, and queues are empty. This timeframe is dedicated to tasks such as patching, upgrades, and configuration. During this timeframe, Avaya Workspaces for Elite and the applications such as Avaya Breeze® platform nodes, System Manager, and Avaya Control Manager remain powered on and accessible on the customer network but does not process any contacts or operations.

** You must delete snapshots from Avaya Oceana® Solution virtual machines before placing Avaya Oceana® Solution back into production.

Configuration and deployment details

The following table lists the configuration and deployment details that you must know before deploying and commissioning the Avaya Workspaces for Elite solution.

Component	Name	Your value
Avaya Aura® Communication Manager	Release	
Avaya Aura® Communication Manager	IP address	
Avaya Aura® Communication Manager	User Name	
Avaya Aura® Communication Manager	Password	

Table continues…

Component	Name	Your value
Avaya Aura® Communication Manager	SAT Password	
Avaya Aura® Communication Manager	Hunt Group number	
Avaya Aura® Communication Manager	CTI-Link number	
Avaya Aura® Communication Manager	VDNs used by Avaya Workspaces for Elite	
Avaya Aura® Communication Manager	Vectors used by Avaya Workspaces for Elite	
Avaya Aura® System Manager	Release	
Avaya Aura® System Manager	Hostname	
Avaya Aura® System Manager	Management IP address	
Avaya Aura® System Manager	LDAP Server IP address	
Avaya Aura® Session Manager	Release	
Avaya Aura® Session Manager	Hostname	
Avaya Aura® Session Manager	Management IP address	
Avaya Aura® Application Enablement Services	Release	
Avaya Aura® Application Enablement Services - Server 1	Hostname	
Avaya Aura® Application Enablement Services - Server 1	Management IP address	
Avaya Aura® Application Enablement Services - Server 1	Switch CTI Link Number	
Avaya Aura® Application Enablement Services - Server 2	Hostname	
Avaya Aura® Application Enablement Services - Server 2	Management IP address	
Avaya Aura® Application Enablement Services - Server 2	Switch CTI Link Number	
Avaya Control Manager	Release	
Avaya Control Manager	Hostname	
Avaya Control Manager	IP address	
Avaya Control Manager	Location	
Avaya Control Manager - Standalone Microsoft SQL Server	IP address	
Avaya Workspaces for Elite cluster 1 - Avaya Breeze® platform node 1	Hostname	
Avaya Workspaces for Elite cluster 1 - Avaya Breeze® platform node 1	Management IP address	

Table continues…

Component	Name	Your value
Avaya Workspaces for Elite cluster 1 - Avaya Breeze® platform node 1	Security IP address	
Avaya Workspaces for Elite cluster 1 - Avaya Breeze® platform node 2	Hostname	
Avaya Workspaces for Elite cluster 1 - Avaya Breeze® platform node 2	Management IP address	
Avaya Workspaces for Elite cluster 1 - Avaya Breeze® platform node 2	Security IP address	
Avaya Workspaces for Elite cluster 1 - Avaya Breeze® platform node 3	Hostname	
Avaya Workspaces for Elite cluster 1 - Avaya Breeze® platform node 3	Management IP address	
Avaya Workspaces for Elite cluster 1 - Avaya Breeze® platform node 3	Security IP address	
Avaya Workspaces for Elite cluster 1	Cluster IP address	
Avaya Workspaces for Elite cluster 1	Primary System Manager IP address	
Avaya Workspaces for Elite cluster 1	Enrollment Password	
Avaya Workspaces for Elite cluster 2 - Avaya Breeze® platform node 1	Hostname	
Avaya Workspaces for Elite cluster 2 - Avaya Breeze® platform node 1	Management IP address	
Avaya Workspaces for Elite cluster 2 - Avaya Breeze® platform node 1	Security IP address	
Avaya Workspaces for Elite cluster 2 - Avaya Breeze® platform node 2	Hostname	
Avaya Workspaces for Elite cluster 2 - Avaya Breeze® platform node 2	Management IP address	
Avaya Workspaces for Elite cluster 2 - Avaya Breeze® platform node 2	Security IP address	
Avaya Workspaces for Elite cluster 2	Cluster IP address	
Avaya Workspaces for Elite cluster 2	Primary System Manager IP address (same value as Avaya Workspaces for Elite cluster 1)	
Avaya Workspaces for Elite cluster 2	Enrollment Password (same value as Avaya Workspaces for Elite cluster 1)	

Chapter 5: Deploy Avaya Breeze® platform nodes

Deploy Avaya Breeze® platform nodes

This section describes how to deploy the Avaya Breeze® platform nodes for both Avaya Workspaces for Elite clusters.

For Avaya Workspaces for Elite solutions that support up to 1000 agents, do not create Avaya Workspaces for Elite Cluster 2. Install the following SVARs on Avaya Workspaces for Elite Cluster 1:

- AuthorizationService
- CallServerConnector
- UCAStoreService
- UCMService
- UnifiedAgentController
- OceanaMonitorService
- CentralizedLoggingService
- MetricbeatService
- PacketbeatService

Note:

For Avaya Workspaces for Elite small solutions, you must configure the Lightweight Directory Access Protocol (LDAP) server certificates for Avaya Workspaces for Elite Cluster 1 nodes only. For Avaya Workspaces for Elite large solutions, you must configure the Lightweight Directory Access Protocol (LDAP) server certificates for Avaya Workspaces for Elite Cluster 2 nodes only.

For Avaya Workspaces for Elite solutions that support up to 7500 agents, install the following SVARs on Avaya Workspaces for Elite Cluster 1:

- CallServerConnector
- UCAStoreService
- UCMService

- OceanaMonitorService
- CentralizedLoggingService
- MetricbeatService
- PacketbeatService

For Avaya Workspaces for Elite solutions that support up to 7500 agents, install the following SVARs on Avaya Workspaces for Elite Cluster 2:

- AuthorizationService
- UnifiedAgentController
- OceanaMonitorService
- MetricbeatService
- PacketbeatService

Important:

To deploy Avaya Breeze® platform nodes and create clusters, you must have sufficient privileges in System Manager. For information about how to manage groups and roles for resources in System Manager, see *Administering Avaya Aura® System Manager*.

Avaya Breeze® platform authorization

When a request is made between a client and a third-party server, an authorization token is passed with the request. The authorization is handled by the Avaya Breeze® platform nodes on the cluster that hosts AuthorizationService. Avaya Workspaces is an example of a client, and Avaya Aura® Device Services is an example of a third-party server. You must import the Avaya Breeze® platform Authorization Certificate on these servers if they are part of your solution.

Each Avaya Breeze® platform node in the cluster has a different Authorization Identity Certificate and when load balancing is enabled between the nodes, some requests can be rejected. Therefore you must first replace the Authorization Identity Certificate on each Avaya Breeze® platform node with a single System Manager-generated Identity Certificate, and then import this common certificate on any servers in your solution that require this Identity Certificate.

This chapter includes procedures describing how to create the common certificate, import it onto Avaya Breeze® platform nodes, and export it from Avaya Breeze® platform.

Avaya Breeze® platform nodes deployment checklist

Use the following checklist to deploy the Avaya Breeze® platform nodes for your Avaya Workspaces for Elite solution:

No.	Task	Notes	✔
1	Download *Deploying Avaya Breeze® platform*	-	

Table continues…

No.	Task	Notes	✔
3	Calculate the number of Avaya Breeze® platform nodes required for your solution	If your planned solution capacity is 1000 agents or less, deploy 3 Avaya Breeze® platform nodes on a Avaya Workspaces for Elite cluster. If your planned solution capacity is more than 1000 agents, deploy 3 Avaya Breeze® platform nodes on Avaya Workspaces for Elite Cluster 1 and deploy 2 Avaya Breeze® platform nodes on Avaya Workspaces for Elite Cluster 2.	
4	Deploy the Avaya Breeze® platform nodes	See *Deploying Avaya Breeze® platform*. If you deploy Avaya Breeze® platform using the OVF template, the default disk size is 50 GB thick-provisioned. Based on your deployment type, you must change the CPU and RAM of Avaya Breeze® platform nodes using the vSphere client. For information about the minimum requirements for Avaya Breeze® platform nodes for each deployment type, see Hardware requirements on page 15. **Important:** These Avaya Breeze® platform nodes are for the exclusive use of the Avaya Workspaces for Elite solution. Do not install any third-party or custom Service Archives (SVARs) on these nodes.	

Verifying the Avaya Breeze® platform deployment using System Manager

About this task

Use this procedure to verify that the Avaya Breeze® platform replication is in sync with System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the Replica Groups page, perform one of the following steps to view the replica nodes for a replica group:
   - Select the replica group and click **View Replica Nodes**.

- Click the replica group name.

3. Verify that **Synchronization Status** for the new Avaya Breeze® platform nodes is `Synchronized`.

   The `Synchronized` status indicates that the system has successfully replicated the data that the replica node requested from the master database to the database of the replica node.

4. **(Optional)** If **Synchronization Status** for a node is not `Synchronized`, then perform the following steps:

   a. Log in to the Avaya Breeze® platform node using an SSH client application, such as PuTTy.

   b. Run the **`AvayaNetSetup`** command.

   c. Review configuration details.

Configuring LDAP server certificates for Avaya Breeze® platform nodes

About this task

Configure the Avaya Breeze® platform nodes to trust your LDAP server certificates. For Avaya Workspaces for Elite small solutions, add the LDAP server certificates to the three Avaya Breeze® platform nodes of Avaya Workspaces for Elite Cluster 1 only. For Avaya Workspaces for Elite large solutions, add the LDAP server certificates to the two Avaya Breeze® platform nodes of Avaya Workspaces for Elite Cluster 2 only.

The clusters do not exist at this point of the deployment. This procedure is intended to prepare the nodes for the cluster configuration.

Before you begin

Add an LDAP server to the solution.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select the check box for one of the nodes of the proposed cluster, and click **More Actions** > **Manage Trusted Certificates**.
3. On the Manage Trusted Certificates page, click **Add**.
4. On the Add Trusted Certificate page, perform the following steps:

   a. Click **Import using TLS**.

   b. In the **IP Address** field, enter the IP address of your LDAP server.

   c. In the **Port** field, enter the port number of your LDAP server.

   d. Click **Retrieve Certificate**.

e. Click **Commit**.

5. Repeat Step 3 to Step 5 for the other nodes of the proposed cluster.

Configuring LDAP server integration

About this task

Avaya Aura® System Manager supports integration with an LDAP authentication server. Therefore, you must configure System Manager to integrate with an LDAP server.

Note:

- This procedure is a basic example of System Manager and LDAP integration. For more information, see *Administering Avaya Aura® System Manager*.
- Avaya Workspaces for Elite only supports secure binding. When you use Active Directory as an LDAP server, you must install a Certificate Authority on the Active Directory server.

Before you begin

Add an LDAP server to the solution.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select the **System Manager** check box, and click **More Actions** > **Manage Trusted Certificates**.
3. On the Manage Trusted Certificates page, click **Add**.
4. On the Add Trusted Certificate page, perform the following steps:
   a. Click **Import using TLS**.
   b. In the **IP Address** field, enter the IP address of your LDAP server.
   c. In the **Port** field, enter the port number as `636`.
   d. Click **Retrieve Certificate**.
   e. Click **Commit**.
5. On the System Manager web console, click **Users** > **Directory Synchronization** > **Sync Users**.
6. On the User Synchronization page, click **New**.
7. On the New User Synchronization Datasource page, in the Directory Parameters section, perform the following steps:
   a. In the **Datasource Name** field, enter the name to identify Active Directory.
   b. In the **Host** field, enter the FQDN address of your LDAP server.

      Ensure that LDAP certificates contain a SAN entry.
   c. In the **Principal** field, enter the LDAP login details.

For example, myDomain\Administrator.

d. In the **Password** field, enter the password for the LDAP login account that you specified.

e. In the **Port** field, enter the port number as `636`.

f. In the **Base Distinguished Name** field, enter the LDAP details.

For example, CN=myDomain.com,DC=myDomain,DC=com

g. In the **Search Filter** field, enter the LDAP search string.

For example, CN=Alex*.

h. Select the **Use SSL** check box.

i. Click **Test Connection**.

8. On the New User Synchronization Datasource page, in the Attribute Parameters section, perform the following steps:

a. Click **Add Mapping** to add a row.

b. From the drop-down list on the left, select **cn**.

c. From the corresponding drop-down list on the right, select **sourceUserKey**.

d. Click **Add Mapping** to add another row.

e. From the drop-down list on the left, select **mail**.

f. From the corresponding drop-down list on the right, select **loginName**.

Note:

Instead of the **mail** field pointing to **loginName**, you also need to use **userPrincipalName** depending on the configuration of the LDAP server. For example, if the **mail** field is not set in the LDAP server.

g. Click **Add Mapping** to add another row.

h. From the drop-down list on the left, select **givenName**.

i. From the corresponding drop-down list on the right, select **surname**.

j. Click **Add Mapping** to add another row.

k. From the drop-down list on the left, select **givenName**.

l. From the corresponding drop-down list on the right, select **givenName**.

m. Click **Add Mapping** to add another row.

n. From the drop-down list on the left, select **givenName**.

o. From the corresponding drop-down list on the right, select **displayName**.

9. Click **Save**.

10. On the User Synchronization page, click **Active Synchronization Jobs**.

11. Click **Create New Job**.
12. On the New User Synchronization Job page, in the **Datasource Name** field, select the LDAP server and click **Run Job**.

    Wait for the job to complete so that all LDAP users are loaded in System Manager.
13. On the User Synchronization page, click **Synchronization Job History**.
14. In the **Status** column, verify that the status of the job is `RUNNING`.

    The status changes to `COMPLETED` when the job is complete.

Avaya Workspaces single sign-on

You can configure Avaya Breeze® platform Authorization Service attributes to enable SAML. The Avaya Breeze® platform Authorization Service also supports IWA/Kerberos authentication.

LDAP integration:

When attempting to access the Avaya Workspaces URL, unauthorized users are redirected to the Avaya Breeze® platform Authorization Service. If LDAP integration is configured, Avaya Breeze® platform prompts the user for credentials. After a successful authentication Avaya Breeze® platform grants users authorization permissions using an authorization token, and if users have the correct permissions set in ACM they can access Avaya Workspaces.

SAML integration:

When attempting to access the Avaya Workspaces URL, unauthorized users are redirected to the Avaya Breeze® platform Authorization Service. If SAML integration is configured, the Authorization Service redirects users to your identity provider (IdP), and prompts the user for credentials. After a successful authentication Avaya Breeze® platform grants users authorization permissions using an authorization token, and if users have the correct permissions set in ACM they can access Avaya Workspaces.

IWA/Kerberos integration:

If the Avaya Breeze® platform Authorization Service is configured for IWA/Kerberos authentication, the Authorization Service automatically uses the Windows credentials of the user for authentication. You do not need to manually enter your credentials when accessing Avaya Workspaces. When attempting to access the Avaya Workspaces URL, users are redirected to the Avaya Breeze® platform Authorization Service, which uses IWA to automatically grant users authorization permissions using an authorization token. If users have the correct permissions set in ACM they can access Avaya Workspaces.

When users exit Avaya Workspaces, they are redirected to the Exit page. Users can choose to immediately return to Avaya Workspaces and if permitted by the Authorization Service, the Activate Agent screen immediately appears and users can log on again without entering credentials.

For more information about Avaya Breeze® platform, SAML, and Kerberos authentication, see Avaya Breeze® platform documentation, available on https://support.avaya.com.

Configuring the WebSphere certificate for Centralized Logging

About this task

To run Centralized Logging in the secure mode, you must configure the WebSphere certificate for each node of the cluster where you plan to install CentralizedLoggingService.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select the check box for the Avaya Breeze® platform node, and click **More Actions** > **Manage Identity Certificates**.
3. On the Manage Identity Certificates page, select **WebSphere** and click **Replace**.
4. On the Replace Identity Certificate page, do the following:
   a. Select the **Replace this Certificate with Internal CA Signed Certificate** option.
   b. In the **Key Algorithm** and **Key Size** fields, select the appropriate values.
   c. In the **Subject Alternative Name** field, select the **IP Address** check box.
   d. In the **IP Address** field, enter the Management IP address of the Avaya Breeze® platform node.
   e. Click **Commit**.
5. Repeat Step 2 to Step 4 for the other nodes.

Creating the common certificate

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, Oceana_Authorization
   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 the cluster that AuthorizationService is installed on.

h. In the first **DNS Name** field, enter the Security Module FQDN for one of the nodes of the cluster.
i. In the second **DNS Name** field, enter the Security Module FQDN for the other node of the cluster.
j. In the **IP Address** field, enter the IP address of the cluster.
k. In the **Token** field, select `P12 file`.
l. 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.

Importing the common certificate in Avaya Breeze® platform nodes

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select the check box for the Avaya Breeze® platform node, and click **More Actions** > **Manage Identity Certificates**.
3. On the Manage Identity Certificates page, select **Authorization** and click **Replace**.
4. On the Replace Identity Certificate page, do the following:
   a. Select the **Import third party certificate** option.
   b. In the **Please select a file (PKCS#12 format)** field, browse and select the common certificate that you generated.
   c. In the **Password** field, enter the password that you specified while creating the end entity.
   d. Click **Commit**.
5. Repeat Step 2 to Step 4 for the other nodes of the cluster.

Exporting the Avaya Breeze® platform Authorization Identity Certificate

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select the check box for any of the Avaya Breeze® platform nodes with the new certificate, and click **More Actions** > **Manage Identity Certificates**.
3. On the Manage Identity Certificates page, select **Authorization** and click **Export**.
4. Save the `.pem` file on your local machine.

Chapter 6: Configure Application Enablement Services

Configure Application Enablement Services

This section provides information about how to configure Application Enablement Services to enable off-the-shelf and custom integration with Avaya Workspaces for Elite.

Application Enablement Services is a set of enhanced telephony APIs, protocols, and Web services. These applications support access to the call processing, media, and administrative features available in Communication Manager.

Configuring Communication Manager Link to Application Enablement Services

About this task

Add a switch connection so that Application Enablement Services can communicate with Communication Manager. After you add a switch connection, you must associate the switch connection name with a procr IP address. Use this procedure when you are setting up a switch connection with a Communication Manager media server that uses a procr connection to Application Enablement Services.

Add a CTI (TSAPI) link between Application Enablement Services and Communication Manager. When adding a CTI (TSAPI) link, the switch CTI link number on Application Enablement Services must match that of the IP Services Server ID for Application Enablement Services as configured in Communication Manager.

Restart the TSAPI connection between Application Enablement Services and Communication Manager. You must restart the TSAPI Service for changes to the CTI link between Application Enablement Services and Communication Manager to take effect.

Note:

If two instances of Application Enablement Services are used for HA, ensure that you repeat all steps for the other AES server. Also, ensure that you configure the other AES server with the same AES user, AES user password, and CM-Name as the first AES server.

Procedure

1. Log in to Application Enablement Services.

2. Click **Communication Manager Interface** > **Switch Connections**.
3. In the Switch Connection page, enter the name of Communication Manager in the text box and click **Add Connection**.

   The system adds the Communication Manager in the list.
4. Select the newly added Communication Manager from the list and click **Edit Connection**.
5. In the **Switch Password** and **Confirm Switch Password** fields, enter the AESVCS password.

   The password must be same as the password on the Communication Manager ip-services configuration.
6. Select the **Processor Ethernet** check box if you are using the Communication Manager procr interface.
7. Click **Apply**.
8. In the Switch Connections page, click **Edit PE/CLAN IPs**.
9. In the Edit Processor Ethernet IP page, enter the IP address of procr and click **Add/Edit Name or IP**.
10. Click **AE Services** > **TSAPI** > **TSAPI Links**.
11. Click **Add Link**.
12. In the Add TSAPI Links section, do the following:
    a. In the **Link** field, select a number which is not already configured.
    b. In the **Switch Connection** field, select the newly added switch connection.
    c. In the **Switch CTI Link Number** field, select the CTI Link number that corresponds to the CTI Link already configured on Communication Manager.
    d. In the **ASAI Link Version** field, select the highest version available.
    e. In the **Security** field, select **Both**.

       You must select **Both** because each TSAPI Link must be configured for both Encrypted and Unencrypted security types.
    f. Click **Apply Changes**.
13. Click **Security** > **Security Database** > **Tlinks**.
14. On the **Tlinks** page, verify that the CSTA and CSTA-S links are added to the system.
15. To restart TSAPI services, perform the following steps:
    a. Click **Maintenance**.
    b. Click **Service Controller**.
    c. Select **TSAPI Service**.
    d. Click **Restart Service**.

16. Click the **Status** > **Status and Control** > **TSAPI Service Summary**.
17. On the TSAPI Link Details page, verify that the status of the TSAPI link is `Talking`.
18. Log in to Communication Manager and run the **`status aesvcs cti-link`** command to check if the CTI links are operational and Service State is `established`.

Configuring AES certificates

Creating an end entity

Procedure

1. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
2. In the left pane, in the RA Functions section, click **Add End Entity**.
3. In the **End Entity Profile** field, select `INBOUND_OUTBOUND_TLS`.
4. In the **Username** field, enter a user name.
5. In the **Password (or Enrollment Code)** field, enter a password.

   For each end entity, the password is mandatory for authentication of the certificate generation request.
6. In the **Confirm Password** field, re-enter the password.
7. Complete any other fields that you want in your certificate.
8. In the **CN, Common name** field, enter the FQDN of the AES server.

   The Common Name is case-sensitive.
9. In the **Certificate Profile** field, select `ID_CLIENT_SERVER`.
10. In the **CA** field, select `tmdefaultca`.
11. In the **Token** field, select `P12 file`.
12. Click **Add**.

    The system displays the `End Entity <username> added successfully` message.

Creating the server certificate

Procedure

1. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
2. In the navigation pane, click **Public Web**.

   This system displays a new browser tab.
3. In the navigation pane, in the Enroll section, click **Create Keystore**.

4. In the **Username** field, enter the user name that you specified while adding an End Entity.
5. In the **Password** field, enter the password that you specified while adding an End Entity.
6. Click **OK**.
7. On the Keystore Enrollment page, perform the following steps:
8. On the EJBCA Token Certificate Enrollment page, select the key length as 2048 and click **Enroll**.
9. Save the server certificate to a known location.

   This is the signed server certificate that you import to Application Enablement Services.

Downloading the CA certificate

Procedure

1. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
2. In the navigation pane, click **Public Web**.

   This system displays a new browser tab.
3. In the navigation pane, in the Retrieve section, click **Fetch CA certificates**.
4. Click **Download PEM chain**.
5. Save the CA certificate.

Importing the CA certificate to Application Enablement Services

Procedure

1. On the Application Enablement Services web console, click **Security** > **Certificate Management** > **CA Trusted Certificates**.
2. Click **Import** and upload the CA certificate you downloaded (PEM file).
3. Specify an alias name. For example, `caSMGR`.
4. Click **Apply**.

Importing the server certificate to Application Enablement Services

Procedure

1. On the Application Enablement Services web console, click **Security** > **Certificate Management** > **Server Certificates**.
2. Click **Import** and upload the server certificate you created.
3. Select **aeservices** from the drop-down menu.
4. Click **Apply**.
5. Enter the password specified while creating the End Entity.
6. Click **Apply**.

7. On the Server Certificate Import page, click **Apply**.

   The server certificate displays in the list on the Server Certificates page.

Creating Application Enablement Services user for Call Server Connector communication

The Call Server Connector (CSC) snap-in is a Voice-only Service Provider interface to the underlying switching infrastructure. CSC provides call control and agent control functions.

In an Avaya Workspaces for Elite solution, CSC communicates with Communication Manager through the Device, Media and Call Control (DMCC) interface in Application Enablement Services. CSC is implemented as a TSAPI application to receive Communication Manager events through Application Enablement Services. CSC uses Application Enablement Services to control and monitor Communication Manager Voice calls and resources.

Before you begin

- Create an Application Enablement Services CT user that has read-write access to User Management features in the Application Enablement Services Management console.
- Create a CT User and CTI User for the CSC snap-in.

Procedure

1. Log on to the Application Enablement Services web console by starting a web browser and entering the following URL:

   `https://<AES_IPaddress>`, where AES_IPaddress is the IP address for the Application Enablement Services server.

2. Click **Continue To Login**.
3. In the **Username** box, type your user name and click **Continue**.
4. In the **Password** box, type your password and click **Continue**.
5. Click **Login**.
6. On the Application Enablement Services web console, navigate to **User Management** > **User Admin**.
7. Click **Add User**.
8. Specify a value for each of the following mandatory fields:
   - **User Id**
   - **Common Name**
   - **Surname**
   - **User Password**
   - **Confirm Password**

- **CT User**: Select `Yes` from the drop-down menu.

9. Click **Apply**.
10. On the Application Enablement Services web console, navigate to **Security** > **Security Database**.
11. Select **CTI Users**.
12. Select **List All Users**.
13. Select the newly added user and click **Edit**.
14. Check the **Unrestricted Access** check box.
15. Click **Apply Changes**.

Verifying Application Enablement Services connection with Call Server Connector service

About this task

Use this procedure to verify that Application Enablement Services is connected to the Call Server Connector (CSC) service.

Procedure

1. On the Application Enablement Services web console, navigate to **Status** > **Status and Control**.
2. Click **DMCC Service Summary**.
3. On the Session Summary page, you see a CSC Primary and a CSC Backup entry for each configured Application Enablement Services/Communication Manager link in CSC. Each entry must have the Far-end identifier same as the IP addresses of the node it is connected to.

   If these sessions are listed, the Application Enablement Services connection to the CSC deployment is successful.

   Note:

   For two standalone instances of Application Enablement Services, CSC connects only to a single AES at any given time.

Chapter 7: Configure Communication Manager resources

Configure Communication Manager resources for Avaya Workspaces for Elite

This section uses a worked example to describe a basic configuration of Communication Manager and Call Center Elite resources for Avaya Workspaces for Elite integration. You can configure these resources as required for your Avaya Workspaces for Elite solution.

Auto answer

Using Communication Manager, you can configure the auto answer setting on the agent or on the station. If enabled for the agent, this overrides the station setting. To use auto answer, the station must be in a service state of *in-service/off-hook*. When you log in to a station using a deskphone, Avaya one-X® Agent, or Avaya Agent for Desktop, the station is in this state. In an Avaya Workspaces for Elite solution, the following auto answer considerations apply when agents start work using Avaya Workspaces for Elite:

- Deskphone
  - If auto answer is enabled on the agent station, the agent cannot Start Work using Avaya Workspaces for Elite. The agent must first press the headset button or remove the deskphone from the cradle. This places the station in the *in-service/off-hook* state that is required for auto answer. Pressing the headset button again or placing the deskphone in the cradle logs the agent out of the station. If the agents wants to end the call using the deskphone without logging out of the station, a release button must be configured on the station.
  - If auto answer is enabled for the agent only, with the station setting disabled, agents can Start Work using Avaya Workspaces for Elite. However, the station is in the *in-service/on-hook* state after agents start work and auto answer is not active. Agents can receive calls which are not automatically answered, and when the call ends the agent is logged out of the station. To enable auto answer, agents must press the headset button or remove the deskphone from the cradle.
  - If auto answer is enabled for both the agent and the station, the agent setting overrides the station setting. However, in this scenario the agent cannot Start Work using Avaya Workspaces for Elite. The agent must first press the headset button or remove the deskphone from the cradle to place the station in the *in-service/off-hook* state that is required for auto answer.

- Avaya one-X® Agent
  - To use auto answer, the **CM Auto Answer Support Required** check box must be selected in Avaya one-X® Agent System Settings.
  - If auto answer is enabled on the agent station, the agent cannot Start Work using Avaya Workspaces for Elite. The agent must first open and expand the dialpad, and click on one of the configured lines. This places a call to the station; when the agent ends this call the station is in the *in-service/off-hook* state that is required for auto answer.
  - If auto answer is enabled for the agent only, with the station setting disabled, agents can Start Work using Avaya Workspaces for Elite. However, the station is in the *in-service/on-hook* state after agents start work and auto answer is not active. Agents can receive a call which is not automatically answered, and when the call ends the station is in the *in-service/off-hook* state that is required for auto answer. All subsequent calls are auto-answered.
  - If auto answer is enabled for both the agent and the station, the agent setting overrides the station setting. However, in this scenario the agent cannot Start Work using Avaya Workspaces for Elite. The agent must first open and expand the dialpad, and click on one of the configured lines. This places a call to the station; when the agent ends this call the station is in the *in-service/off-hook* state that is required for auto answer.
- Avaya Agent for Desktop
  - To use auto answer, the **CM Auto Answer Support Required** check box must be selected on the **Preferences** tab in Avaya Agent Configuration.
  - If auto answer is enabled on the agent station, the agent cannot Start Work using Avaya Workspaces for Elite. The agent must first dial ‘0’. When the agent ends this call the station is in the *in-service/off-hook* state that is required for auto answer.
  - If auto answer is enabled for the agent only, with the station setting disabled, agents can Start Work using Avaya Workspaces for Elite. However, the station is in the *in-service/on-hook* state after agents start work and auto answer is not active. Agents can receive a call which is not automatically answered, and when the call ends the station is in the *in-service/off-hook* state that is required for auto answer. All subsequent calls are auto-answered.
  - If auto answer is enabled for both the agent and the station, the agent setting overrides the station setting. However, in this scenario the agent cannot Start Work using Avaya Workspaces for Elite. The agent must first dial ‘0’. When the agent ends this call the station is in the *in-service/off-hook* state that is required for auto answer.

Logging on to Communication Manager

About this task

Log on to Avaya Aura® Communication Manager to configure parameters and resources for integration with Avaya Workspaces for Elite.

Procedure

1. Using an SSH client such as PuTTY, begin an SSH session using the Communication Manager IP address.

2. Click **Open**.
3. When prompted enter the user name and password for the Communication Manager.
4. Press return to ignore terminal selection and when prompted for high priority session, enter `n`.
5. To access the System Access Terminal (SAT), type `sat` and enter the same password used above.
6. When prompted, enter a preferred terminal type. For example, select the w2ktt Terminal Emulator.

Configuring System Features and Customer Options

About this task

On the Communication Manager System Parameters Features form, verify that Universal Call Identifier (UCID) is enabled. UCID is an Avaya proprietary call identifier used to help correlate call records between different systems. UCID must also be configured on the Trunk Group to Avaya Aura® Session Manager.

Procedure

1. Run **`change system-parameters features`**.
2. On page 5 of the FEATURE-RELATED SYSTEM PARAMETERS screen, in the **UNIVERSAL CALL ID** field, perform the following steps:
   a. Set the **Create Universal Call ID (UCID)** field to `y`.
   b. Set the **UCID Network Node ID** field to *any unique node id number*.
3. On page 11 of the system-parameters feature screen, set the **Expert Agent Selection (EAS) Enabled?** field to `y`.
4. On page 13 of the system-parameters feature screen, set the **Send UCID to ASAI** field to `y`.
5. Save the settings.
6. Run **`change system-parameters customer-options`**.
7. On page 10 of the ASAI PROPRIETARY FEATURES screen, verify that the **Proprietary?** field is set to `y`.

   Note:

   You must use material code 232301 to activate the Proprietary features, for example Agent States.
8. Save the settings.

Configuring Signaling and Trunk Groups

About this task

Using Communication Manager, you create Signaling and Trunk Groups for the trunk between Session Manager and Communication Manager. You must configure Universal Call Identifier (UCID) on the Signaling and Trunk Groups.

Procedure

1. Run **`change signaling-group n`**.

   n is the number of the Signaling Group that you need to specify.

2. On page 1 of the SIGNALING GROUP screen, perform the following steps:

   a. Set the **Initial IP-IP Direct Media?** field to `y`.

   b. Set the **Session Establishment Timer (min)** field to `65`.

3. Save the settings.
4. Ensure that UUI is enabled on any trunks configured so that incoming calls to an Avaya Workspaces for Elite VDN contain the Agent ID as UUI.
5. Run **`change trunk-group n`**.

   n is the number of the Trunk Group that you need to specify.

6. On page 3 of the TRUNK FEATURES screen, perform the following steps:

   a. Set the **UUI Treatment** field to `shared`.

   b. Set the **Send UCID?** field to `y`.

7. On page 4 of the SHARED UUI FEATURE PRIORITIES screen, ensure that the **ASAI**, **UCID**, and **Collected Digits** fields are not blank.
8. Save the settings.

Configuring a Route Pattern

About this task

After configuring the Signaling and Trunk Groups, you must configure a Route Pattern on Communication Manager.

Before you begin

Ensure that you identify the Route Pattern that you want to configure.

Procedure

1. Run **`change route-pattern n`**.

n is the number of the Route Pattern that you want to configure. The assumption is that there are existing Route Patterns created in Communication Manager.

2. On page 1 of the route-pattern screen, perform the following steps:
   a. In the **Pattern Name** field, enter a name for the Route Pattern.
   b. In the **Grp No** field, enter the previously-configured Trunk Group number.
   c. In the **FRL** field, enter the appropriate FRL.
3. Save the settings.

Adding a Route Pattern to the Locations table

About this task

After configuring a Route Pattern, you must add the Route Pattern to the Locations table on Communication Manager.

Before you begin

Ensure that you identify the Route Pattern that you want to add to the Locations table.

Procedure

1. Run **`change locations`**.
2. On page 1 of the LOCATIONS screen, in the **Proxy Sel Rte Pat** field, enter the previously-configured Route Pattern number.
3. Save the settings.

Configuring CTI-Link to Application Enablement Services

About this task

On Communication Manager, configure IP Services for the Application Enablement Services (AES) transport link and then add a CTI-Link from Communication Manager to the AES server. The other end of this CTI-Link is configured on the AES server.

Procedure

1. Run **`change node-names ip`**.
2. Make an entry for the AES host name and IP address in the respective fields and save the entry.

   The host name must match the host name on the AES server.
3. Save the settings.
4. Run **`change ip-services`**.

5. On page 1 of the IP SERVICES screen, perform the following steps:
   a. In the **Service Type** field, add `AESVCS`.
   b. In the **Enabled** field, set the value to `y`.
   c. In the **Local Node** field, enter `procr`.
   d. In the **Local Port** field, verify that 8765 is the default port.
6. On page 3 of the AE Services Administration screen, perform the following steps:
   a. In the **AE Services Server** field, enter the AES host name.

      The host name must match the host name on the AES server.
   b. In the **Password** field, enter a password.

      The password must have 12 to 16 characters.
   c. In the **Enabled** field, set the value to `y`.
7. Save the settings.
8. Run **`add cti-link next`** or **`add cti-link n`**.

   n is the number of cti-link that you must use.
9. On page 1 of the CTI LINK screen, perform the following steps:
   a. In the **Extension** field, enter a valid extension.
   b. In the **Name** field, enter the name of the AES server.
   c. In the **Type** field, set the type to `ADJ-IP`.
10. On page 2 of the CTI LINK screen, in the **IC Adjunct Routing** field, set the value to `y`.
11. Save the settings.

Configuring Direct Agent Calling

About this task

Communication Manager uses the Direct Agent Calling (DAC) for the Class of Restriction (COR).

DAC is required for RONA to work. With this setting enabled, you cannot make a direct call using an AgentID if the agent is in an AUX (NR) Not Ready state. When this setting is disabled, you can make a direct call using an AgentID regardless of agent state but RONA does not work correctly.

Procedure

1. Run **`change COR n`**.

   n is the number of COR being used on Communication Manager.
2. Set the **Direct Agent Calling** field to `y`.
3. Save the settings.

Configuring a Hunt Group for Avaya Workspaces for Elite

About this task

Configure Hunt Groups for your Avaya Workspaces for Elite solution, so that calls can route to Avaya Workspaces for Elite agents. You can add multiple Hunt Groups for your Avaya Workspaces for Elite solution.

Procedure

1. Run **`add hunt-group next`** or **`add hunt-group n`**.

   n is the number of the hunt group that you need to specify. For example, 1001.

2. On page 1 of the HUNT GROUP screen, perform the following steps:
   a. In the **Group Number** field, enter the number of the Hunt Group.
   b. In the **Group Name** field, enter the name of the Hunt Group. For example, use `WorkspacesElite`.
   c. In the **Group Extension** field, enter the extension number for this Hunt Group.
   d. Set the **ACD** field to `y`.
   e. Set the **Queue** field to `y`.
   f. Set the **Vector** field to `y`.
3. On page 2 of the HUNT GROUP screen, perform the following steps:
   a. Set the **Skill** field to `y`.
   b. Set the **Timed ACW Interval** field to the required number of seconds for your solution. This sets the number of seconds Avaya Workspaces for Elite agents remain in After Contact Work after completing a call.
4. On page 3 of the HUNT GROUP screen, perform the following steps:
   a. Set the **Redirect on No Answer (rings)** field to the required value for your solution.

      The value must specify the number of unanswered rings before the call is redirected.

   b. Set the **Redirect on No Answer to VDN** field to the required value for your solution.

      For this basic example, the call redirects to a VDN (3011). In this scenario, you can route the call to any configured VDN.
5. Save the settings.

Example

```
display hunt-group 1001                                        Page   1 of   4
                                  HUNT GROUP

           Group Number: 1001                               ACD? y
             Group Name: WorkspacesElite                  Queue? y
        Group Extension: 3009                            Vector? y
             Group Type: ucd-mia
                     TN: 1
                    COR: 1                        MM Early Answer? n
          Security Code:                    Local Agent Preference? n
 ISDN/SIP Caller Display:

            Queue Limit: unlimited
 Calls Warning Threshold:      Port:
  Time Warning Threshold:      Port:
```

```
display hunt-group 1001                                        Page   2 of   4
                                  HUNT GROUP

                  Skill? y      Expected Call Handling Time (sec): 180
                    AAS? n        Service Level Target (% in sec): 80 in 20
               Measured: external
    Supervisor Extension:


     Controlling Adjunct: none



  Multiple Call Handling: none

Timed ACW Interval (sec): 10       After Xfer or Held Call Drops? n
```

```
display hunt-group 1001                                        Page   3 of   4
                                    HUNT GROUP

             Interruptible Aux Threshold: none


      Redirect on No Answer (rings): 3
       Redirect on No Answer to VDN: 3011          Retain Active VDN Context? n
Redirect on IP/OPTIM Failure to VDN:
Forced Entry of Stroke Counts or Call Work Codes? n
```

Creating variables using Communication Manager

About this task

Communication Manager vectors use variables to improve efficiency. Different types of variables are available to meet different types of call processing needs. Vector variables can be added to consider location, messaging, and adjunct routing vector steps. Based on the variable type, variables can use call-specific data or fixed values that are identical for all calls. In either case, an administered variable can be reused in many vectors.

In this example, vector C is used to collect 5 digits and assign these digits to vector D as User-to-User Information (UUI) data.

If the variables used in this example are already in use on Communication Manager, use different variables. Ensure that you use these different variables in your Avaya Workspaces for Elite vectors.

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Use the **`change variables`** command.
3. On page 1 of the Variables for Vectors screen, perform the following steps for variable C:
   a. In the **Description** field, enter the description of the variable C as `Digits`.
   b. In the **Type** field, enter the value `collect`.

c. In the **Scope** field, enter the value `L`.

The value L specifies the Local variable.

d. In the **Length** field, enter the value `5`.

e. In the **Start** field, enter the value `1`.

This value specifies the digit start position.

f. Save variable C.

4. On page 1 of the Variables for Vectors screen, perform the following steps for variable D:

a. In the **Description** field, enter the description of the variable D as `UUI-info`.

b. In the **Type** field, enter the value `asaiuui`.

c. In the **Scope** field, enter the value `L`.

The value L specifies the Local variable.

d. In the **Length** field, enter the value `5`.

e. In the **Start** field, enter the value `1`.

This value specifies the digit start position.

f. Save variable D.

5. Add any further variables as required for your solution.

6. Save the settings.

Example

```
display variables                                          Page   1 of  39
                              VARIABLES FOR VECTORS

Var Description                Type    Scope Length Start Assignment       VAC
A   Adjunct Route Digits       collect L     16     1
B   Adjunct Route Flag         collect P     1      1
C   digits                     collect L     5      1
D   UUI-info                   asaiuui L     5      1
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
```

Configuring VDN's and vectors for Avaya Workspaces for Elite

About this task

Use this procedure to configure basic VDN's and vectors which you can use to route calls to Avaya Workspaces for Elite agents.

Procedure

1. Run **`add vdn next or add vdn n`**.

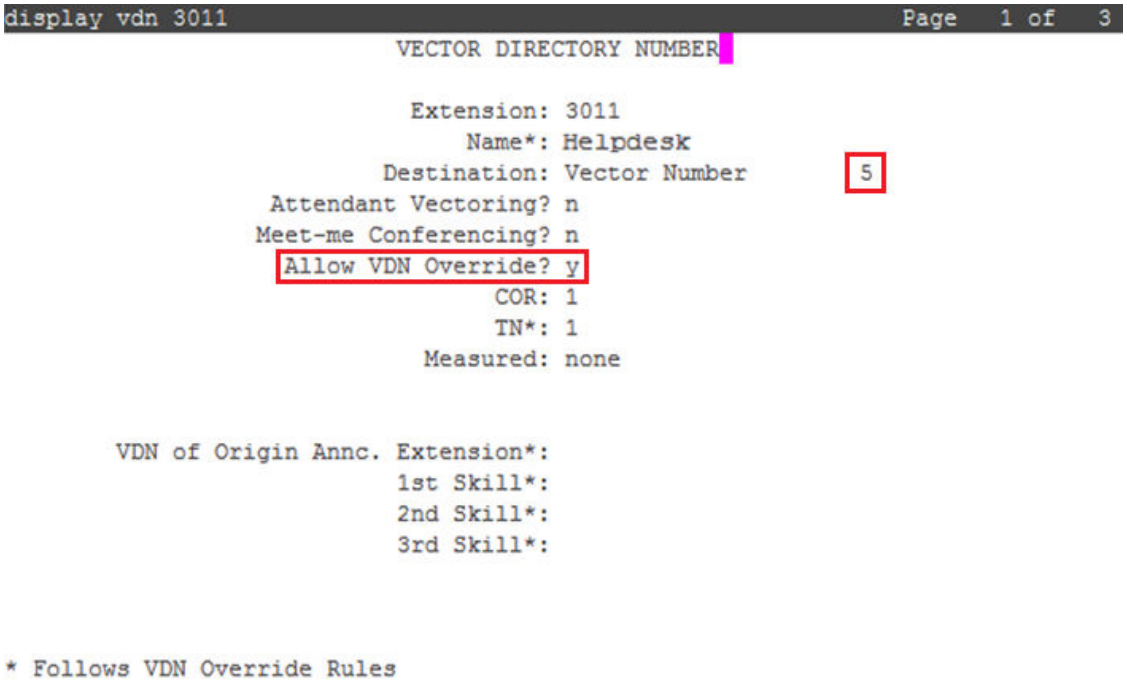
   n is the extension that you want to use for the VDN. This example uses 3011.

2. On page 1 of the VECTOR DIRECTORY NUMBER screen, perform the following steps:

   a. In the **Name** field, enter the name of the VDN.

   b. In the **Destination** field, set the destination to a vector number which is not in use. This example uses 5.

   c. In the **Allow VDN Override** field, type `y`. This allows this VDN to be overridden and routed to another VDN.



   d. Save the settings.

3. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.

4. Run **`change vector n`**.

   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Routing VDN. In this example, the vector number is 5.

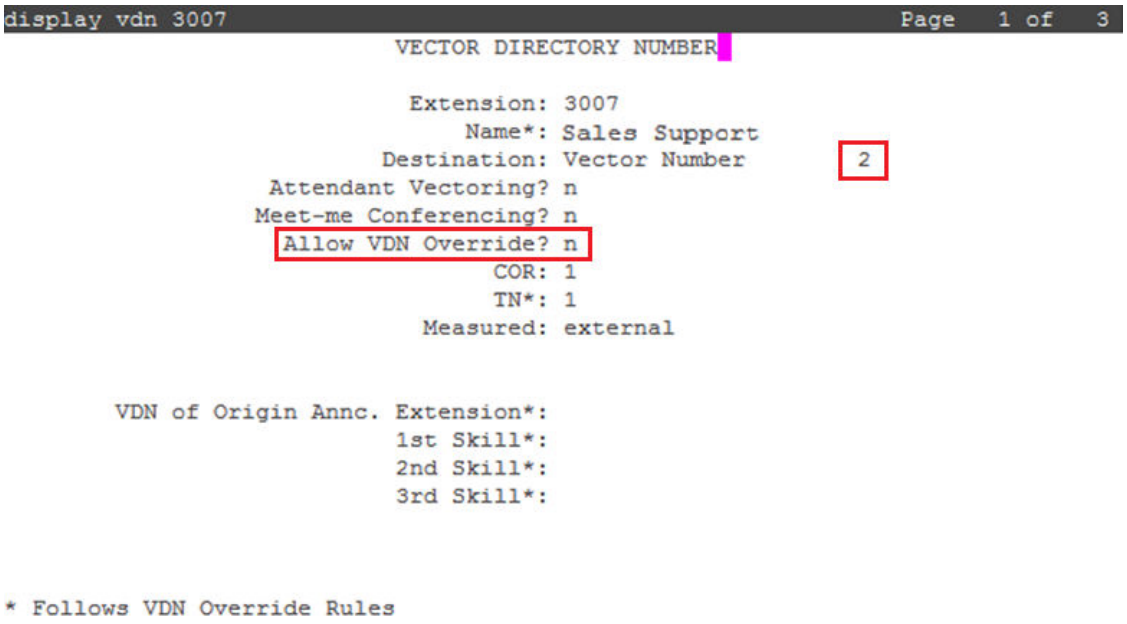
5. On page 1 of the CALL VECTOR screen, perform the following steps:
   a. In the **Name** field, enter the name of the vector.
   b. Enter the details required from line 01 to line 03 as shown below. This is an example of a basic vector which routes the call to another VDN:

```
display vector 5                                          Page   1 of   6
                                CALL VECTOR

    Number: 5                Name: Helpdesk
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 route-to     number 3007             with cov n if unconditionally
03 stop
04
05
06
07
08
09
10
11
12

                        Press 'Esc f 6' for Vector Editing
```

   c. Save the settings.
6. Run **`add vdn next or add vdn n`**.

   n is the extension that you want to use for the VDN. This example uses 3007.
7. On page 1 of the VECTOR DIRECTORY NUMBER screen, perform the following steps:
   a. In the **Name** field, enter the name of the VDN.
   b. In the **Destination** field, set the destination to a vector number which is not in use. This example uses 2.

c. In the **Allow VDN Override** field, type `n`.



d. Save the settings.

8. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
9. Run **`change vector n`**.

   n is the number that you entered in the **Destination** field of the VECTOR DIRECTORY NUMBER screen while creating the Routing VDN. In this example, the vector number is 2.
10. On page 1 of the CALL VECTOR screen, perform the following steps:
    a. In the **Name** field, enter the name of the vector.
    b. Enter the details required from line 01 to line 05 as shown below. This is an example of a basic vector which collects digits and assigns the digits to variable C. The

collected digits are set to Variable D. The call then routes to the Avaya Workspaces for Elite Hunt Group:

```
display vector 2                                          Page   1 of   6
                                CALL VECTOR

    Number: 2                Name: Sales Support
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 collect      5    digits after announcement none     for C
03 set          D      = digits SEL   5
04 route-to     number 3009             with cov n if unconditionally
05 stop
06
07
08
09
10
11
12

                        Press 'Esc f 6' for Vector Editing
```

c. Save the settings.

Configuring Agent Login ID using Communication Manager

About this task

Use this procedure to configure Agent position IDs.

Note:

Using Communication Manager, you can configure the auto answer setting on the agent or on the station. If enabled for the agent, this overrides the station setting. To use the station setting, ensure that the agent Auto Answer setting is set to station.

To use auto answer, the station must be in a service state of *in-service/off-hook*.

Procedure

1. Run **`add agent-loginID next`** or **`add agent-loginID agent-loginID`**.

   agent-loginID is based on the individual Communication Manager dial plan.

2. On page 1 of the AGENT LOGINID screen, perform the following steps:

   a. In the **Login ID** field, enter the login ID of the agent based on the individual Communication Manager dial plan.

   b. In the **Name** field, enter a representative name for the Agent.

   c. In the Auto Answer field, configure the setting to one of the following values as required for your solution: `all`, `acd`, `none`, or `station`.

3. On page 2 of the AGENT LOGINID screen, perform the following steps:
   a. In the **Direct Agent Skill** field, enter the Hunt Group number that you created.
   b. In Row 1, type the previous Hunt Group number in the **SN** field and type `1` in the **SL** field.
4. Save the settings.

Configuring Agent Phone-sets

About this task

Use this procedure to configure agent phones to support Avaya Workspaces for Elite.

Procedure

1. Configure agent phones to support the following Call Center Elite capabilities:
   - Call Appearance

     Avaya Workspaces for Elite requires three Call Appearance lines on each agent station.
   - Login
   - Logout
   - Auto-in / Manual-in
   - Aux Work
   - After Call (optional)
2. For each SIP User station, ensure that the **Type of 3PCC Enabled** field is set to `Avaya`.
3. For each SIP User station, ensure the **Trunk Selection** field for the phone extension is `aar`.

Adding AUX codes

About this task

In a Call Center Elite solution, agents can enter Auxiliary Work (AUX) mode using different reason codes. Agents set these AUX codes using their phones.

In Avaya Workspaces, codes used before and after handling contacts are called user codes. For example, enter a user code while changing state, or before going on a break, an agent can use a user code configured to represent break time.

If an agent sets an AUX code using their phone, this is reflected on Avaya Workspaces. If an agent uses Avaya Workspaces to set a user code, this code is also set on Call Center Elite and can be reported on by Call Management System (CMS). In an Avaya Workspaces for Elite solution, agent states and reason codes are always synchronized between agent phones and Avaya Workspaces.

Use this procedure to add AUX codes on Communication Manager. Call Center Elite supports single digit or two digit AUX codes.

Important:

You must also configure AUX codes in Avaya Control Manager to ensure the AUX codes are synchronized to UCA. If no AUX codes exist in UCA, agents cannot go Not Ready in Avaya Workspaces. For more information about configuring AUX codes in Avaya Control Manager, see Configuring AUX codes on page 89.

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. If you want to add AUX codes with two digits, perform the following steps:
   a. Use the **`change system-parameters features`** command, and ensure that the **Two-Digit Aux Work Reason Codes?** field is set to **y**:

```
change system-parameters features                              Page  14 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
REASON CODES
                          Aux Work Reason Code Type: forced
                            Logout Reason Code Type: none
                      Two-Digit Aux Work Reason Codes? y
     Redirection on No Answer Aux Work Reason Code: 5
ROOF Failure and Unreachable Aux Work Reason Code: 8

REDIRECTION ON IP CONNECTIVITY FAILURE
                 Switch Hook Query Response Timeout: 5000
                    IP Failure Aux Work Reason Code: 9

MAXIMUM AGENT OCCUPANCY PARAMETERS
                 Maximum Agent Occupancy Percentage: 100
      Maximum Agent Occupancy Aux Work Reason Code: 9
```

   b. Save the settings.
   c. Use the **`change cti-link`** command, and ensure that the **Two-Digit Aux Work Reason Codes?** field is set to **y**:

      Important:

      You must busy out the cti-link before changing this field. Ensure that you release the cti-link after you save your changes.

```
change cti-link 1                                          Page   2 of   3
                                    CTI LINK
FEATURE OPTIONS

      Event Minimization? n          Special Character for Restricted Number? n
      IC Adjunct Routing? n    Send Disconnect Event for Bridged Appearance? n
                                        Two-Digit Aux Work Reason Codes? y
                                             Block CMS Move Agent Events? n
                                             Remove '+' from SIP Numbers? y
```

d. Save the settings.

3. To add AUX codes, use the **`change reason-code-names`** command.
4. On page 1 of the REASON CODE NAMES screen, enter names for the AUX codes as required.
5. Save the settings.

Example

```
change reason-code-names                                   Page   1 of   3

                              REASON CODE NAMES

                          Aux Work/              Logout
                        Interruptible?

        Reason Code 1: Bathroom          /n
        Reason Code 2: Breakfast         /n
        Reason Code 3: Lunch             /n
        Reason Code 4: Dinner            /n
        Reason Code 5: RONA              /n
        Reason Code 6: Training          /n
        Reason Code 7: Meeting           /n
        Reason Code 8: ROOF              /n
        Reason Code 9: ROIF              /n

  Default Reason Code: Default
```

Configuring auto answer

About this task

Using Communication Manager, you can configure the auto answer setting on the agent or on the station. If enabled for the agent, this overrides the station setting. You can configure the agent auto answer setting to use the auto answer value set on the agent station.

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. To enable auto answer for an agent, use the **`change agent-loginID n`** command where *n* is the agent ID. On page 1 of the AGENT LOGINID screen, set the auto answer field to one of the following values:
   - `all`: Enter `all` to immediately send all ACD and non-ACD calls to the agent. The station is also given a single ring while a non-ACD call is connected. The ringer-off button can be used to prevent the ring when, on the Feature-Related System Parameters screen, the Allow Ringer-off with Auto-Answer field is set to `y`.
   - `acd`: Enter `acd` to allow only ACD split/skill calls and direct agent calls to auto answer. If this field is set to `acd`, non-ACD calls terminated to the agent ring audibly.
   - `none`: all calls terminated to this agent receive an audible ringing treatment. This is the default setting.
   - `station`: auto answer for the agent is controlled by the auto answer field on the station that the agent has logged in on.

```
change agent-loginID 3419                                    Page   1 of   3
                                AGENT LOGINID

               Login ID: 3419                                    AAS? n
                   Name: Indira Varma                          AUDIX? n
                     TN: 1        Check skill TNs to match agent TN? n
                    COR: 1
        Coverage Path:                                 LWC Reception: spe
        Security Code:                           LWC Log External Calls? n
        Attribute:                          AUDIX Name for Messaging:

                                       LoginID for ISDN/SIP Display? n
                                                           Password: 1234
                                               Password (enter again): 1234
                                                       Auto Answer: station
                                                  MIA Across Skills: system
                                           ACW Agent Considered Idle: system
                                           Aux Work Reason Code Type: system
                                             Logout Reason Code Type: system
                                 Maximum time agent in ACW before logout (sec): none
                                                  Forced Agent Logout Time:  :
WARNING:  Agent must log in again before changes take effect
```

3. Save the settings.
4. To enable auto answer on a station, use the **change station n** command where *n* is the station number. On page 2 of the STATION screen, set the auto answer field to one of the following values:
   - `all`: Enter `all` to allow ACD and non-ACD calls terminated to an idle station to be cut through immediately. For non-ACD calls, the set is also rung while the call is cut through. The ring can be prevented by activating the ringer-off feature button when, on the Feature-Related System Parameters screen, the Allow Ringer-off with Auto-Answer field is set to `y`.
   - `acd`: Enter `acd` to allow only ACD split/skill calls and direct agent calls to auto answer. If this field is set to `acd`, non-ACD calls terminated to a station ring audibly.
   - `none`: all calls terminated to this agent receive an audible ringing treatment. This is the default setting.

```
change station 3219                                    Page   2 of   5
                                    STATION
FEATURE OPTIONS
           LWC Reception: spe                 Auto Select Any Idle Appearance? n
          LWC Activation? y                             Coverage Msg Retrieval? y
  LWC Log External Calls? n                                   Auto Answer: all
            CDR Privacy? n                                Data Restriction? n
   Redirect Notification? y                       Idle Appearance Preference? n
 Per Button Ring Control? n                     Bridged Idle Line Preference? n
   Bridged Call Alerting? n                         Restrict Last Appearance? y
  Active Station Ringing: single
                                                          EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number? _
      Service Link Mode: as-needed                    EC500 State: enabled
        Multimedia Mode: enhanced                 Audible Message Waiting? n
    MWI Served User Type:                       Display Client Redirection? n
            AUDIX Name:                       Select Last Used Appearance? n
                                                Coverage After Forwarding? s
                                                 Multimedia Early Answer? n
Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
 Emergency Location Ext: 3219          Always Use? n IP Audio Hairpinning? n
    Precedence Call Waiting? n
```

5. Save the settings.

Configuring auto-in and manual-in station buttons

About this task

If you enable manual-in, agents must manually change to Ready after ending a call and exiting after call work (ACW). If you enable auto-in, agents automatically go Ready after ending a call and exiting after call work (ACW).

In an Avaya Workspaces for Elite solution, the default behavior is auto-in. If you want to use the manual-in option you must add a manual-in button to agent stations. If you want to use both the auto-in and manual-in options, you must also add an auto-in button.

Important:

You must also enable manual-in using Avaya Workspaces settings. If agents are using deskphones, they can use the deskphone to set manual-in or auto-in. However, the manual-in setting in Avaya Workspaces settings must still be selected. Avaya Workspaces for Elite does not support setting manual-in using Avaya one-X® Agent or Avaya Agent for Desktop. Agents must use Avaya Workspaces to set manual-in, and you must ensure that the manual-in option is not enabled in Avaya one-X® Agent or Avaya Agent for Desktop. For more information about Avaya Workspaces settings, see *Using Avaya Workspaces for Elite.*

Procedure

1. Use the **`change station n`** command where *n* is the station number. On page 4 of the STATION screen, add the buttons as required for your solution.

```
change station 3219                                    Page   4 of   5
                                    STATION
 SITE DATA
      Room:                                          Headset? n
      Jack:                                          Speaker? n
     Cable:                                         Mounting: d
     Floor:                                     Cord Length: 0
  Building:                                       Set Color:

ABBREVIATED DIALING
     List1:                List2:                List3:


BUTTON ASSIGNMENTS
 1: call-appr                          5: release
 2: call-appr                          6: aux-work      RC:   Grp:
 3: call-appr                          7: after-call          Grp:
 4: manual-in          Grp:            8: auto-in             Grp:

    voice-mail
```

2. Save the settings.

Chapter 8: Deploy clusters

Deploy Avaya Workspaces for Elite clusters

The Avaya Workspaces for Elite solution includes the following clusters:

- Avaya Workspaces for Elite Cluster 1
- Avaya Workspaces for Elite Cluster 2

Important:

These clusters are for the exclusive use of the Avaya Workspaces for Elite solution. Do not install any third-party or custom Service Archives (SVARs) on this cluster.

For Avaya Workspaces for Elite solutions that support up to 1000 agents, do not create Avaya Workspaces for Elite Cluster 2. Install the following SVARs on Avaya Workspaces for Elite Cluster 1:

- AuthorizationService
- CallServerConnector
- UCAStoreService
- UCMService
- UnifiedAgentController
- OceanaMonitorService
- CentralizedLoggingService
- MetricbeatService
- PacketbeatService

For Avaya Workspaces for Elite solutions that support up to 7500 agents, install the following SVARs on Avaya Workspaces for Elite Cluster 1:

- CallServerConnector
- UCAStoreService
- UCMService
- OceanaMonitorService
- CentralizedLoggingService

- MetricbeatService
- PacketbeatService

For Avaya Workspaces for Elite solutions that support up to 7500 agents, install the following SVARs on Avaya Workspaces for Elite Cluster 2:

- AuthorizationService
- UnifiedAgentController
- OceanaMonitorService
- MetricbeatService
- PacketbeatService

A cluster provides scaling by distributing the services across multiple Avaya Breeze® platform nodes. With this distribution of services, the system achieves overall throughput and avoids interruption in the event of failure. Clients access the services through a Cluster IP address that supports High Availability (HA).

Verifying host name resolution for Avaya Breeze® platform nodes

About this task

Use this procedure to verify that the Avaya Breeze® platform nodes host names can be resolved.

Procedure

1. Register the fully qualified domain names (FQDNs) of the following servers and virtual machines with a Domain Name System (DNS) server:
   - System Manager
   - Avaya Workspaces for Elite Cluster 1 IP address and FQDN
   - Avaya Workspaces for Elite Cluster 2 IP address and FQDN
   - Avaya Breeze® platform node host names
   - Avaya Breeze® platform security IP addresses

   Important:

   - If you do not complete this step, Avaya Breeze® platform replication does not synchronize for each node. Failure to synchronize prevents the deployment from completing.
   - The returned DNS record is case-sensitive. Therefore, it must exactly match the node.
2. Verify that System Manager can resolve the host name of Avaya Breeze® platform nodes.

Loading license files in System Manager

About this task

Use this procedure to load the license files for Avaya Breeze® platform nodes and services that are used by Avaya Workspaces.

Procedure

1. On the System Manager web console, click **Services** > **Licenses**.
2. Click **Install License**.
3. On the Install License page, perform the following steps:
   a. Browse to the location of the license that you want to install and select the license file.
   b. Click **Accept the License Terms & Conditions**.
   c. Click **Install**.

      The system installs the license.
4. In the left pane, click **Licensed Products** to view the installed license.
5. Perform steps 2 through 4 to install the license for the following services:
   - COLLABORATION_ENVIRONMENT (For the Avaya Breeze® platform)
   - Avaya_Oceana
6. In the left pane, click **WebLM Home** to verify that the WebLM Home page displays all the licenses.
7. After the services are running, perform the following steps to verify the licenses:
   a. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
   b. On the Services page, verify that the **License Mode** column for all the services displays a check mark.

Loading SVARs in System Manager

About this task

Use this procedure to load the following Avaya Breeze® platform Service Archive (SVARs) of the Avaya Workspaces for Elite clusters in System Manager:

Cluster name	SVAR
Avaya Workspaces for Elite Cluster 1	• CallServerConnector • UCAStoreService • UCMService • CentralizedLoggingService • OceanaMonitorService • MetricbeatService • PacketbeatService
Avaya Workspaces for Elite Cluster 2	• AuthorizationService • UnifiedAgentController • OceanaMonitorService • MetricbeatService • PacketbeatService

Note:

For Avaya Workspaces for Elite solutions that support up to 1000 agents, you must load all of the SVARs on Avaya Workspaces for Elite Cluster 1.

Before you begin

- Remove the older SVAR versions.
- Download the latest SVAR versions.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. On the Services page, click **Load**.
3. In the Load Service dialog box, do the following:
   a. Click **Browse**.
   b. Select the SVAR and click **Open**.
   c. To load multiple SVARs at the same time, repeat steps a and b for each SVAR.

      Note:

      You can select up to 50 files or a maximum file size of 3 GB.

   d. Click **Load**.
4. In the Accept End User License Agreement dialog box, click **Accept**.

   If you load multiple SVARs at the same time, you must click **Accept** for each SVAR.
5. On the Services page, verify that the state of the SVARs is `Loaded`.

Creating Avaya Workspaces for Elite Cluster 1

About this task

Use this procedure to create Avaya Workspaces for Elite Cluster 1.

Note:

Do not add nodes to the cluster while performing this procedure.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, click **New**.
3. On the Cluster Editor page, select the **General** tab.
4. In the Basic section, perform the following steps:
   a. In the **Cluster Profile** field, select **Customer Engagement**.
   b. In the **Cluster Name** field, enter a unique cluster name.

      The name must be a string of Alphanumeric characters. For example, `AvayaWorkspacesEliteCluster1`.
   c. In the **Cluster Group** field, select a cluster group.

      Important:

      Ensure that you do not use the selected cluster group for any non-Avaya Workspaces for Elite cluster.
   d. In the **Cluster IP** field, enter the IP address of the cluster.

      The IP address of the cluster must be on the same subnet as the Security Module IP address of the Avaya Breeze® platform nodes that you plan to add to the cluster.

      Ensure that you do not specify the IP address of any of the Avaya Breeze® platform nodes that you plan to add to the cluster.

      The system uses the IP address of the cluster as the load balancer. The system does not provide an option to select Avaya Breeze® platform instances within the cluster for load balancing.
   e. In the **Cluster Fully Qualified Domain Name** field, enter the FQDN of the cluster.
   f. Select the **Enable Cluster Database** check box.
   g. Select the **Enable Database Auto Switchover** check box.
   h. In the **Description** field, enter a description for the cluster.
5. In the Cluster Attributes section, perform the following steps:
   a. In the **Authorization Services Address** field, enter the FQDN of the cluster that hosts the Authorization service.

b. Increase the value of the attribute **Http or Https limit on connections** per client from the default value of 100, so that the cluster supports more connections simultaneously.

   The suggested value is 6000.

c. Select or clear the **Only allow secure web communications** check box as required for your solution.

d. Clear the **Is load balancer enabled** check box.

   Important:

   After adding Avaya Breeze® platform nodes to the cluster, you must edit the cluster and select this check box.

e. Clear the **Is session affinity enabled** check box.

f. In the **Default SIP Domain** field, enter the default SIP domain for the cluster.

For more information about Cluster Attributes, see *Administering Avaya Breeze® platform*.

6. On the Cluster Editor page, select the **Services** tab.

   The system automatically adds CallEventControl and EventingConnector SVARs to the Assigned Services list.

7. In the Available Services list, click the plus sign **(+)** to add the following SVARs to Avaya Workspaces for Elite Cluster 1:

   - CallServerConnector
   - UCAStoreService
   - UCMService
   - CentralizedLoggingService
   - OceanaMonitorService
   - MetricbeatService
   - PacketbeatService

   For Avaya Workspaces for Elite solutions that support up to 1000 agents, you must also add the following SVARs to Avaya Workspaces for Elite Cluster 1:

   - AuthorizationService
   - UnifiedAgentController

8. Click **Commit**.

   The system prompts you to ensure that you restart all Avaya Breeze® platform nodes before placing the cluster into the Accept New Service state.

9. Click **OK**.

Creating Avaya Workspaces for Elite Cluster 2

About this task

Use this procedure to create Avaya Workspaces for Elite Cluster 2.

Note:

- For Avaya Workspaces for Elite solutions that support up to 1000 agents, this procedure does not apply.
- Do not add nodes to the cluster while performing this procedure.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, click **New**.
3. On the Cluster Editor page, select the **General** tab.
4. In the Basic section, perform the following steps:
   a. In the **Cluster Profile** field, select **Customer Engagement**.
   b. In the **Cluster Name** field, enter a unique cluster name.

      The name must be a string of Alphanumeric characters. For example, `AvayaWorkspacesEliteCluster2`.
   c. In the **Cluster Group** field, select a cluster group.

      Important:

      Ensure that you do not use the selected cluster group for any non-Avaya Workspaces for Elite cluster.
   d. In the **Cluster IP** field, enter the IP address of the cluster.

      The IP address of the cluster must be on the same subnet as the Security Module IP address of the Avaya Breeze® platform nodes that you plan to add to the cluster.

      Ensure that you do not specify the IP address of any of the Avaya Breeze® platform nodes that you plan to add to the cluster.

      The system uses the IP address of the cluster as the load balancer. The system does not provide an option to select Avaya Breeze® platform instances within the cluster for load balancing.
   e. In the **Cluster Fully Qualified Domain Name** field, enter the FQDN of the cluster.
   f. Select the **Enable Cluster Database** check box.
   g. Select the **Enable Database Auto Switchover** check box.
   h. In the **Description** field, enter a description for the cluster.

5. In the Cluster Attributes section, perform the following steps:
   a. In the **Authorization Services Address** field, enter the FQDN of the cluster that hosts the Authorization service.
   b. Increase the value of the attribute **Http or Https limit on connections** per client from the default value of 100, so that the cluster supports more connections simultaneously.

      The suggested value is 6000.
   c. Select or clear the **Only allow secure web communications** check box as required for your solution.
   d. Clear the **Is load balancer enabled** check box.

      Important:

      After adding Avaya Breeze® platform nodes to the cluster, you must edit the cluster and select this check box.
   e. Clear the **Is session affinity enabled** check box.
   f. In the **Default SIP Domain** field, enter the default SIP domain for the cluster.

   For more information about Cluster Attributes, see *Administering Avaya Breeze® platform*.
6. On the Cluster Editor page, select the **Services** tab.

   The system automatically adds CallEventControl and EventingConnector SVARs to the Assigned Services list.
7. In the Available Services list, click the plus sign **(+)** to add the following SVARs to Avaya Workspaces for Elite Cluster 2:
   - AuthorizationService
   - UnifiedAgentController
   - OceanaMonitorService
8. Click **Commit**.

   The system prompts you to ensure that you restart all Avaya Breeze® platform nodes before placing the cluster into the Accept New Service state.
9. Click **OK**.

Setting cluster services attributes

About this task

Use this procedure to configure the attributes of each SVAR installed on Avaya Workspaces for Elite clusters.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. To configure CallServerConnector, on the Service Clusters tab, do the following:
    a. In the **Cluster** field, select the Avaya Workspaces for Elite cluster.
    b. In the **Service** field, select **CallServerConnector**.
    c. For **Solution type**, select the **Override Default** check box and select **Elite** from the drop-down list.
    d. For **Deployment type**, select the **Override Default** check box and select **ELITE_SMALL** or **ELITE_LARGE** from the drop-down list, depending on your solution capacity.
    e. For **Deploy CSC**, select the **Override Default** check box and select **true** from the drop-down list.
    f. For **Voice Provider Id**, select the **Override Default** check box and type the name of the Voice provider that you plan to configure in Avaya Control Manager. Ensure that the value entered is of type CM, for example type CM3436. This setting is case-sensitive.
    g. For **Application Enablement Services' IP addresses**, select the **Override Default** check box and type the IP address of the Application Enablement Services server that you plan to connect to Communication Manager using a TSAPI link. If you use two instances of Application Enablement Services for HA, click the plus sign (+) and add the second instance.
    h. For **Application Enablement Services User**, select the **Override Default** check box and type the Application Enablement Services user name. If you use two instances of Application Enablement Services for HA, you must configure the same user name for both instances.
    i. For **Application Enablement Services User Password**, select the **Override Default** check box and type the Application Enablement Services user name password. If you use two instances of Application Enablement Services for HA, you must configure the same password for both instances.
    j. For **Communication Manager Connection Name on Application Enablement Services**, select the **Override Default** check box and type the name of the Communication Manager switch connection that you plan to configure on Application Enablement Services. For example type CM3436. This setting is case-sensitive. If you use two instances of Application Enablement Services for HA, you must configure the same name for both instances.
    k. Click **Commit**.
3. To configure UCMService, on the Service Clusters tab, do the following:
    a. In the **Cluster** field, select the Avaya Workspaces for Elite cluster.
    b. In the **Service** field, select **UCMService**.

c. For **Deployment type**, select the **Override Default** check box and select **ELITE_SMALL** or **ELITE_LARGE** from the drop-down list, depending on your solution capacity.

d. For **Enable Secure Communications**, select the **Override Default** check box and select **true** or **false** from the drop-down list to enable or disable secure communications.

e. Click **Commit**.

4. To configure UCAStoreService, on the Service Clusters tab, do the following:

a. In the **Cluster** field, select the Avaya Workspaces for Elite cluster.

b. In the **Service** field, select **UCAStoreService**.

c. For **Deployment type**, select the **Override Default** check box and select **ELITE_SMALL** or **ELITE_LARGE** from the drop-down list, depending on your solution capacity.

d. For **Oceana persistence configuration**, select the **Override Default** check box and select **ELITE_DATABASE** from the drop-down list.

e. Under **Advanced**, for **Enable Tokenless Access**, select the **Override Default** check box and select **TRUE**.

f. Click **Commit**.

g. On the warning dialog box, click **OK**.

5. To configure UnifiedAgentController, on the Service Clusters tab, do the following:

a. In the **Cluster** field, select the Avaya Workspaces for Elite cluster.

b. In the **Service** field, select **UnifiedAgentController**.

c. For **Deployment type**, select the **Override Default** check box and select **ELITE_SMALL** or **ELITE_LARGE** from the drop-down list, depending on your solution capacity.

d. For **Enable Secure Communications**, select the **Override Default** check box and select **true** or **false** from the drop-down list to enable or disable secure communications.

e. For **UCA Cluster**, select the **Override Default** check box and select the Avaya Workspaces for Elite cluster from the drop-down list.

f. For **UCM Cluster**, select the **Override Default** check box and select the Avaya Workspaces for Elite cluster from the drop-down list.

g. Click **Commit**.

h. On the warning dialog box, click **OK**.

6. To configure AuthorizationService, on the Service Clusters tab, do the following:

a. In the **Cluster** field, select the Avaya Workspaces for Elite cluster.

b. In the **Service** field, select **AuthorizationService**.

c. For **UCA Cluster**, select the **Override Default** check box and select the Avaya Workspaces for Elite cluster from the drop-down list.

d. Click **Commit**.

7. To configure OceanaMonitorService, on the Service Clusters tab, do the following:

a. In the **Cluster** field, select the Avaya Workspaces for Elite cluster.

b. In the **Service** field, select **OceanaMonitorService**.

c. For **Cluster 1**, select the **Override Default** check box and depending on the size of your solution, select Avaya Workspaces for Elite Cluster 1 or Avaya Workspaces for Elite Cluster 2 from the drop-down list.

d. For **Secure Connection**, select the **Override Default** check box and select **true** or **false** from the drop-down list to enable or disable secure communications.

e. Click **Commit**.

8. To configure CentralizedLoggingService, on the Service Clusters tab, do the following:

a. In the **Cluster** field, select the Avaya Workspaces for Elite cluster.

b. In the **Service** field, select **CentralizedLoggingService**.

c. For each of the **Days To Retain Logs** settings, select the **Override Default** check box and type the number of days for which the logs must be retained in the index. The system deletes the logs that are older than the number of days specified in these fields.

d. For **Kibana User name**, select the **Override Default** check box and type the user name to log in to the Kibana user interface.

e. For **Kibana user password**, select the **Override Default** check box and type the passowrd to log in to the Kibana user interface.

f. For **Logstash security**, select the **Override Default** check box and select **true** or **false** from the drop-down list to enable or disable the security (SSL) mode for the Logstash service.

g. For each of the **Maximum Log Space(in GB)** settings, select the **Override Default** check box and type the maximum permissible log space for the logs in the index. This value is in GB. The system deletes the older logs after the space specified in this field is occupied.

h. Click **Commit**.

9. To configure MetricbeatService, on the Service Clusters tab, do the following:

a. In the **Cluster** field, select the Avaya Workspaces for Elite cluster.

b. In the **Service** field, select **MetricbeatService**.

c. For **Enable module - system**, if the effective value is set to **false**, select the **Override Default** check box and in the **Effective Value** field select **true**.

d. Click **Commit**.

Adding nodes to Avaya Workspaces for Elite cluster 1

About this task

This procedure describes how to add the required Avaya Breeze® platform nodes to Avaya Workspaces for Elite cluster 1.

You install the CentralizedLoggingService Avaya Workspaces for Elite cluster 1. Therefore, you must identify the WebSphere and Security Module HTTPS certificates for all Avaya Breeze® platform nodes on Avaya Workspaces for Elite cluster 1 and ensure that the certificates are signed by the same Certificate Authority (CA). You must also ensure that these certificates have a different Common Name (CN).

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, select the check box for the cluster and click **Edit**.
3. On the Cluster Editor page, select the **Servers** tab.

   The Avaya Breeze® platform nodes appear under Unassigned Servers.
4. Under Unassigned Servers, click the plus sign **(+)** on each of the three Avaya Breeze® platform nodes to add to the Avaya Workspaces for Elite cluster.

   The three Avaya Breeze® platform nodes appear under Assigned Servers.

   Important:

   Do not add additional Avaya Breeze® platform nodes to the cluster.
5. On the Cluster Editor page, select the **General** tab.
6. Select the **Is load balancer enabled** check box.
7. Click **Commit**.

   The system prompts you to ensure that you restart all Avaya Breeze® platform nodes before placing the cluster into the Accept New Service state.
8. Click **OK**.
9. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
10. On the Cluster Administration page, click **Show** on the new cluster to verify whether the nodes were added to the cluster.
11. On System Manager, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
12. On the Services page, verify that the state of the Avaya Workspaces for Elite SVARs is `Installing`.

    The state changes to `Installed` when the installation completes.
13. When the service installation completes, restart the three Avaya Breeze® platform nodes.

Adding nodes to Avaya Workspaces for Elite cluster 2

About this task

This procedure describes how to add the required Avaya Breeze® platform nodes to Avaya Workspaces for Elite cluster 2.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, select the check box for the cluster and click **Edit**.
3. On the Cluster Editor page, select the **Servers** tab.

   The Avaya Breeze® platform nodes appear under Unassigned Servers.
4. Under Unassigned Servers, click the plus sign **(+)** on each of the two Avaya Breeze® platform nodes to add to the Avaya Workspaces for Elite cluster.

   The two Avaya Breeze® platform nodes appear under Assigned Servers.

   Important:

   Do not add additional Avaya Breeze® platform nodes to the cluster.
5. On the Cluster Editor page, select the **General** tab.
6. Select the **Is load balancer enabled** check box.
7. Click **Commit**.

   The system prompts you to ensure that you restart all Avaya Breeze® platform nodes before placing the cluster into the Accept New Service state.
8. Click **OK**.
9. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
10. On the Cluster Administration page, click **Show** on the new cluster to verify whether the nodes were added to the cluster.
11. On System Manager, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
12. On the Services page, verify that the state of the Avaya Workspaces for Elite SVARs is `Installing`.

    The state changes to `Installed` when the installation completes.
13. When the service installation completes, restart the three Avaya Breeze® platform nodes.

Verifying the status of Avaya Breeze® platform nodes

About this task

Verify the status of Avaya Breeze® platform nodes. For detailed information, see *Deploying Avaya Breeze® platform*.

Procedure

1. Identify the Avaya Breeze® platform nodes where you want to install the snap-in services.
2. On the System Manager web console, navigate to **Services** > **Replication** and verify that all Avaya Breeze® platform nodes are in the synchronized state.
3. Perform the following steps to verify that all Avaya Breeze® platform nodes pass the maintenance tests:
    a. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **System Tools and Monitoring** > **Maintenance Tests**.
    b. In the **Select Avaya Breeze to test** field, select the Avaya Breeze® platform node for which you want to perform maintenance tests.
    c. Click **Execute All Tests**.
    d. Verify that the **Test Result** column for all tests displays the result as `Success`.
    e. Repeat step b through d for the other Avaya Breeze® platform nodes.
4. Perform the following steps to check the system state of all Avaya Breeze® platform nodes:
    a. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Server Administration**.
    b. Ensure that the **System State** column for all Avaya Breeze® platform nodes displays the state as `Denying`.

Setting Cluster State to Accepting

About this task

Use this procedure to set the cluster state of all clusters to Accepting, so that they can accept http or https requests.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. Select the check box for Avaya Workspaces for Elite Cluster 1.
3. In the **Cluster State** field, select **Accept New Service**.
4. In the Warning: Accept New Service dialog box, click **Continue**.
5. Verify that the Cluster State column for the cluster displays `Accepting [x/x]`.

6. Repeat Step 2 to Step 5 for Avaya Workspaces for Elite Cluster 2 if required.

Enabling CORS for clusters

About this task

Use this procedure to enable Cross-origin Resource Sharing (CORS) for Avaya Oceana® Cluster 1 and Avaya Oceana® Cluster 2. CORS is a mechanism by which restricted resources on a node can be requested from another domain outside the domain from which the resource originated.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **HTTP Security**.
2. On the HTTP Security page, perform the following steps:
   a. In the **Cluster** field, select the cluster.
   b. Select the **HTTP CORS** tab.
   c. Select the **Allow Cross-origin Resource Sharing for all** check box.
   d. Click **Commit**.

Certificate-based authentication

For certificate-based authentication, you must perform the following procedures using the System Manager web portal:

1. Configure the client certificate challenge in Avaya Breeze® platform Element Manager.

   The configuration is available on the **Avaya Breeze®** > **Configuration** > **HTTP Security** page.
2. Create a client keystore.
3. Download the Avaya Breeze® platform trusted certificate from System Manager.
4. Authenticate browsers.

Ensure that client applications that access the snap-in operations provide the location and credentials of the client certificate and trusted certificate to establish a secure session with the cluster.

For information about Avaya Breeze® platform certificate-based authentication, see the *Security* chapter in *Avaya Breeze® platform Overview and Specification*.

For information about Avaya Aura® System Manager certificate-based authentication, see the *Security Enhancement* section in *Avaya Aura® System Manager Overview and Specification*.

Verifying Application Enablement Services connection with Call Server Connector service

About this task

Use this procedure to verify that Application Enablement Services is connected to Call Server Connector (CSC).

Procedure

1. On the Application Enablement Services web console, navigate to **Status** > **Status and Control**.
2. Click **DMCC Service Summary**.
3. On the Session Summary page, you see a CSC Primary and a CSC Backup entry for each configured Application Enablement Services/Communication Manager link in CSC. Each entry must have the Far-end identifier which match the IP addresses of the node it is connected to.

   If these sessions are listed, the Application Enablement Services connection to the CSC deployment is successful.

   Note:

   If you have two standalone instances of Application Enablement Services, CSC connects only to a single AES at any given time.

Installing the Authorization Identity Certificate on the cluster

About this task

Use the following procedure to configure the Avaya Breeze® platform Authorization identity certificates on the Avaya Workspaces for Elite cluster.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, select the check box for the Avaya Workspaces for Elite cluster.
3. Click on the **Certificate Management** drop-down list, and select **Update/Install Identity Certificate (Authorization Service)**.

Viewing Oceana Monitor Service pages

About this task

The Oceana Monitor Service includes two pages that provide you with information about the status of the clusters and services in your Avaya Workspaces for Elite solution.

The Oceana Services Overview page provides the following information about each snap-in in your Avaya Workspaces for Elite solution:

- Name of the snap-in
- Symbol specifying whether Oceana Monitor Service has detected the snap-in
  - The ✔ symbol indicates that Oceana Monitor Service has detected the snap-in.
  - The ✖ symbol indicates that Oceana Monitor Service has not detected the snap-in.
- Version of the snap-in
- Name of the cluster where the snap-in is installed
- Latest Heartbeat message of the snap-in

  The Heartbeat message includes the node reporting the Heartbeat, the status level of the Heartbeat (OK, WARN, ERROR), and the time since the last update. Heartbeat background indicates the status of the Heartbeat.

The Monitor Service page provides the following information about the Avaya Workspaces for Elite cluster:

- Name of the cluster
- IP address of the cluster
- Number of nodes in the cluster
- IP address of each node of the cluster
- Cluster view of the snap-ins installed
- View of snap-in lifecycle messages

When you click the cluster node, the Monitor Service page displays the following buttons:

Button name	Description
Show Node Details	Displays information about the nodes of the cluster.

Table continues…

Button name	Description
Show Grid Info	Displays the following information about the processing units of the cluster: • Name of the processing unit • Embedded space of the processing unit • Number of instances • Type of the processing unit • Status of the processing unit
Show Cluster Messages	Displays the service messages for all the snap-ins installed on the cluster.
Show Service Details	Displays the following information about each of the snap-ins installed on the cluster: • Name of the snap-in • Version of the snap-in • Service messages of the snap-in

This procedure describes how to access the Overview and Monitor Service pages.

Procedure

1. To access the Monitor Service page, in your web browser, enter the following URL:

   `https://<Cluster IP>/services/OceanaMonitorService/monitor.html`

2. Do one of the following:
   - If the **Authorization Required to view Monitor output** attribute of OceanaMonitorService is set to `true`, log in to the Authorization Service page.
   - If the **Authorization Required to view Monitor output** attribute of OceanaMonitorService is set to `false`, go to Step 3.
3. On the Monitor Service page, click the cluster node to view the information about the cluster.
4. To access the Oceana Services Overview page, in your web browser, enter the following URL:

   `https://<Cluster IP>/services/OceanaMonitorService/services.html`

Rebooting the Avaya Workspaces for Elite cluster

About this task

This procedure describes how to reboot the Avaya Workspaces for Elite cluster after you have performed all required cluster deployment and configuration tasks.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, select the check box for the Avaya Workspaces for Elite cluster.
3. Click **Reboot**.

   A reboot is possible only if the cluster is in a Denying state. You must ensure that you set the cluster to the Accepting state after the reboot.

Chapter 9: Commission Avaya Workspaces for Elite

Commission Avaya Workspaces for Elite

This section describes how to commission your Avaya Workspaces for Elite Solution using Avaya Control Manager and System Manager.

For more information about how to install and initially configure Avaya Control Manager, see *Installing Avaya Control Manager for Enterprise* and *Configuring Avaya Control Manager*.

Creating a Communication Manager user for Avaya Control Manager

About this task

Using the Communication Manager web interface, add a Communication Manager user for use by Avaya Control Manager.

Procedure

1. In your web browser, enter the following URL to open the Communication Manager web console:

   `http://<CM IP address or FQDN>`

2. Click **Administration** > **Server (Maintenance)** > **Security** > **Administrator Accounts**.
3. Select **Privileged Administrator**.
4. Click **Submit**.

   Note:

   The Communication Manager account is used when adding Communication Manager in the Avaya Control Manager config.

   The system displays the Administrator Login - Add Login screen.

5. In the **Login name** field, enter an administrator login name.

The login name:

- Can have alphabetic characters
- Can have numbers
- Can have an underscore (_)
- Cannot have more than 31 characters

6. In the **Primary group** field, enter `susers` for a privileged login.
7. In the **Additional group (profile)** field, add an access profile.

   The system automatically populates the values in the Linux shell and the Home directory fields.
8. In the **Enter password** field, enter the password for the login.
9. In the **Re-enter password** field, re-enter the same password.
10. **(Optional)** To change the password after the first login, in the **Force password/key change on next login** field, select **yes**.
11. Click **Submit**.

Logging in to Avaya Control Manager

About this task

Use this procedure to log in to Avaya Control Manager to administer Avaya Workspaces for Elite resources.

Before you begin

Install SSL certificates on the Avaya Control Manager server. For more information, see Avaya Control Manager documentation.

Procedure

1. In your web browser, enter the following URL:

   `https://<acccm_hostmame>/ACCCMPortal`

   <acccm_hostname> is the host name of the Avaya Control Manager server.
2. On the Avaya Control Manager login page, perform the following steps:
   a. In the **Username** field, enter the user name.

      The initial user name is `itnv`.
   b. In the **Password** field, enter the password.

      The initial password is `itnv`.
   c. Click **Login**.

      The system prompts you to change the password.

3. Change the password.
4. Log in to Avaya Control Manager using your new credentials.
5. If you receive any errors in Internet Explorer trying to connect to the ACCCM tiles, add the Avaya Control Manager IP address to the local hosts file.

Creating a location for Avaya Workspaces for Elite

About this task

Use this procedure to create a location in Avaya Control Manager for your Avaya Workspaces for Elite solution.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Locations**.
2. On the Location List page, click **Add**.
3. On the Location Add page, perform the following steps:
   a. In the **Name** field, type the name of the location.
   b. In the **Description** field, type the description of the location.
   c. **(Optional)** In the **Auditing Location** field, leave the value as `False` or select `True` to activate audit logging for the location.
   d. Click **Save**.

Adding Communication Manager to Avaya Control Manager

About this task

Use this procedure to add the Communication Manager used in your Avaya Workspaces for Elite solution to Avaya Control Manager.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Team Engagement**.
2. On the Team Engagement page, select **Communication Manager**.
3. On the Communication Manager List page, click **Add**.
4. On the Communication Manager Edit page, do the following:
   a. In the **CM Alias Name** field, enter the alias name of Communication Manager.
   b. In the **CM IP Address** field, enter the IP address of Communication Manager.
   c. In the **CMS ACD** field, type `1`.
   d. In the **CM Username** field, enter the user name of the Privileged Administrator account that you created earlier.

e. In the **CM Password** field, enter the password of the Privileged Administrator account that you created earlier.

f. In the **CM Type** field, select `S8700`.

g. In the **CM Version** field, select the supported version of Communication Manager.

h. In the **Terminal Type** field, select `ossi3`.

i. In the **Is Pin Required** field, select `Yes` or `No` based on your requirement.

j. In the **CM PIN** field, type the PIN code of the user that Control Manager uses for Communication Manager integration.

k. In the **CM Port** field, type the port number that is used for Communication Manager integration. The default port number is `5022` for SSH integration.

l. In the **Time Of Day tables number** field, type `32`.

m. In the **Time Zone** field, select the time zone where the Communication Manager system is located.

n. Click **Save**.

The Communication Manager List page displays the entry for the Communication Manager.

Adding Communication Manager to the Avaya Workspaces for Elite location

About this task

Use this procedure to add the Communication Manager created for the Avaya Workspaces for Elite solution to the Avaya Control Manager location.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Locations**.
2. On the Location List page, select the location created for Avaya Workspaces for Elite.
3. Click **Edit**.
4. On the Location Edit page, select the **Systems** tab.
5. Click the **+** sign.
6. In the **System Type** field, select **CM**.

   The **System Name** field populates the name of the newly created Communication Manager.
7. Leave the **Sync Schedule** field blank and click **Save**.
8. Click **Confirm** on the Warning message dialog box.

Assigning the Avaya Workspaces for Elite location to UCA Proxy Server

About this task

Use this procedure only if Avaya Control Manager services are segregated based on Avaya Control Manager locations.

Before you begin

Ensure that the Avaya Workspaces for Elite clusters are in a running and accepting state.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Services** > **UCA Proxy**.
3. On the UCA Proxy Server List page, perform the following steps:
   a. Select the UCA Proxy Server to which you want to assign a location.
   b. Click **Edit**, or double-click the location.
4. On the UCA Proxy Server Edit page, perform the following steps:
   a. Select the **Location** tab.
   b. Move the required location from the **Available locations** list to the **Selected locations** list.

      Ensure that you move the location that contains the UCA server to the relevant Avaya Control Manager services.
   c. Click **Save**.

Assigning the Avaya Workspaces for Elite location to Application Server

About this task

Use this procedure only if Avaya Control Manager services are segregated based on Avaya Control Manager locations.

Before you begin

Ensure that the Avaya Workspaces for Elite clusters are in a running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Services** > **Application Server**.

2. On the Application Server List page, perform the following steps:
    a. Select the Application Server to which you want to assign a location.
    b. Click **Edit**.
3. On the Application Server Edit page, perform the following steps:
    a. Select the **Location** tab.
    b. Move the required location from the **Available locations** list to the **Selected locations** list.

       Ensure that you move the location that contains the UCA server to the relevant Avaya Control Manager services.
    c. Click **Save**.

Assigning the Avaya Workspaces for Elite location to Synchronizer Service Server

About this task

Use this procedure only if Avaya Control Manager services are segregated based on Avaya Control Manager locations.

Before you begin

Ensure that the Avaya Workspaces for Elite clusters are in a running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Services** > **Synchronizer**.
2. On the Synchronize Services List page, perform the following steps:
    a. Select the Synchronizer Service Server to which you want to assign a location.
    b. Click **Edit**.
3. On the Synchronize Service Edit page, perform the following steps:
    a. Select the **Location** tab.
    b. Move the required location from the **Available locations** list to the **Selected locations** list.

       Ensure that you move the location that contains the UCA server to the relevant Avaya Control Manager services.
    c. Click **Save**.

Adding site, department, and team to Avaya Control Manager

About this task

Use this procedure to add the site, department and team information in the organization tree. The organizational tree manages users, sites, departments, and teams in an organizational chart.

The following are the organizational hierarchy level:

- Site
- Department
- Team

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.
3. In the left pane, click **Organization tree**.
4. Click the  button next to the **Add** button.
5. Click the **Add Organization Chart Items**  button.
6. On the Site tab, enter the information in the following fields:
   a. In the **Site Name** field, enter a name for the site.
   b. In the **Site description** field, enter a description for the site.
   c. In the **Site location** field, select the Communication Manager that you created in the previous procedures.
   d. Click **Save**.
   e. Click **Close**.
7. In the left pane, click the newly created site.
8. Click the  button next to the **Add** button.
9. Click the **Add Organization Chart Items**  button.
10. On the Department tab, enter the information in the following fields:
    a. In the **Department name** field, enter a name for the department.
    b. In the **Department site** field, select the site that you created.
    c. In the **Department description** field, enter a description for the department.
    d. Click **Save**.
    e. Click **Close**.

11. In the left pane, click the newly created department.
12. Click the  button next to the **Add** button.
13. Click the  button.
14. On the Team tab, enter the information in the following fields:
    a. In the **Team name** field, enter a name for the team.
    b. In the **Team department** field, select the department that you created.
    c. In the **Team description** field, enter a description for the team.
    d. Select the **Default Sync Team** check box.
    e. Click **Save**.
    f. Click **Close**.

Synchronizing Avaya Control Manager and Communication Manager

About this task

Use the following procedure to synchronize configuration data from Communication Manager to the Avaya Control Manager database.

Important:

- Use this initial synchronization process only once. If you use this process multiple times, all data is synchronized to the Avaya Control Manager database again and duplicate rows appear.
- This procedure must be performed on the Avaya Control Manager server.

Procedure

1. Log in to the Avaya Control Manager server.
2. On the Avaya Control Manager server, go to the `<install_path>\Avaya\Avaya Control Manager <version>\Services\ACCCM Synchronizer` folder.
3. Right-click the `NAV360_Synchronizer` file and click **Run as administrator**.
4. Click **Start** to start the synchronization process.
5. Click **Yes** on the confirmation screen.
6. After the synchronization process is complete, perform the following steps to verify that resources successfully synchronized to Avaya Control Manager:
    a. On the Avaya Control Manager webpage, click **Users**.
    b. Select the **Users** tab.

c. In the left pane, select the site created previously.

d. Verify that the users created on Communication Manager are available in the right pane.

Creating an Avaya Workspaces for Elite server

About this task

Unified Collaboration Administration (UCA) is an Avaya Breeze® platform service that stores the static administration data for the Avaya Workspaces for Elite solution. You can use Avaya Control Manager to add agent, attribute, provider, and resource information to the Avaya Breeze® platform components used in the Avaya Workspaces for Elite solution.

Use the following procedure to create the Avaya Workspaces for Elite server in Avaya Control Manager.

Procedure

1. Log on to the Avaya Control Manager interface with administrator credentials.
2. On the Avaya Control Manager webpage, click **Configuration** > **Customer Engagement** > **Workspaces for Elite**.
3. On the Workspaces for Elite Server List page, click **Add**.
4. In the **Alias** field, type an alias name for the server.
5. In the **API URL** field, type the URL of the UCA REST interface.

   For example, `https://<WorkspacesForEliteCluster_IP>/services/UCAStoreService/uca`.
6. In the **Version** field, select the Avaya Workspaces for Elite release version.
7. Click **Save**.

Adding the Avaya Workspaces for Elite server to the Avaya Workspaces for Elite location

About this task

Add the Avaya Workspaces for Elite server to a Control Manager location.

Before you begin

Ensure that the Avaya Workspaces for Elite clusters are in a running and accepting state.

Procedure

1. Log on to the Avaya Control Manager interface with administrator credentials.
2. On the Avaya Control Manager webpage, click **Configuration** > **Locations**.

3. On the Location List page, select the location where you want to add the Avaya Workspaces for Elite server.
4. Click **Edit**, or double-click the location.
5. On the Location Edit page, select the **Systems** tab.
6. Click the **+** sign.
7. In the **System Type** field, select **Workspaces for Elite**.

   The **System Name** field populates the name of the newly created Avaya Workspaces for Elite server.
8. Click **Save**.
9. Click **Confirm** on the Warning message dialog box.

Configuring the Avaya Workspaces for Elite server

About this task

Use the following procedure to configure the Avaya Workspaces for Elite URL connection information for Avaya Control Manager. This procedure also synchronizes the Elite VDN and Skill details to the Avaya Workspaces for Elite server. These details are then available to Avaya Workspaces when a contact is presented to an agent.

Procedure

1. Log on to the Avaya Control Manager interface with administrator credentials.
2. On the Avaya Control Manager webpage, click **Configuration** > **Customer Engagement** > **Workspaces for Elite**.
3. Select the Avaya Workspaces for Elite server and click **Edit**.
4. Select the **Communication Manager** tab.
5. To add the Communication Manager used in your Avaya Workspaces for Elite solution, perform the following steps:
   a. Click **Add Provider**.
   b. In the **Name** field, type the same name as the providerId value that you entered when creating the CSC attributes in the Communication Manager list.
6. Click on the **Save Provider** icon.

   The data is synchronized to the Avaya Workspaces for Elite server.
7. Select the **Communication Manager** tab.
8. In the **Voice mail Access** field, type the number to access the voice mail system. Agents can dial this number using the voice mail icon in Avaya Workspaces.
9. In the **External Access Code** field, type the number to make an external voice call. Avaya Workspaces prefixes this number when an agent makes an external call.

10. Click on the **Save Provider** icon.
11. Select the **System Properties** tab.
12. Expand the **Workspaces** section.
13. Under **General**, in the **Avaya Workspaces Welcome Page URL** field, type the URL for an optional web page that presents to Avaya Workspaces agents when they log in.
14. Under **Global Screenpop Behaviours**, perform the following steps:
    a. Select the **Launch external Screen-pops on Agent Accept** check box to open external screenpops in new browser windows when an interaction is answered.
    b. Select the **Display internal Screen-pops Widget first on Agent Accept** check box to display the screenpop widget instead of the contact type widget when an agent accepts an interaction.
15. Under **Supervisor**, perform the following steps:
    a. Select the **Supervisor Can Modify Agent State** check box to permit all supervisors to modify the state of the agent when the agent is not active on a contact.
    b. In the **Supervisor Reporting Dashboard URL** field, type the URL of the web page that presents to supervisors.
16. Under **Widget Library** , perform the following steps:
    a. Select the **Enable An External Widget Library** check to enable the external widget library to include additional widgets in Avaya Workspaces.
    b. In the **Workspaces Library URL** field, type the URL of the external widget library that you want to load in Avaya Workspaces.
17. Under **Avaya Workforce Optimization Select (AWFOS)**, select the **Avaya Work Force Optimization Select Enabled** check box to indicate that Avaya Workforce Optimization Select is available as part of the deployment.
18. Click **Save**.

Configuring AUX codes

About this task

In a Call Center Elite solution, agents can enter Auxiliary Work (AUX) mode using different reason codes. Agents set these AUX codes using their phones.

In Avaya Workspaces, codes used before and after handling contacts are called user codes. For example, enter a user code while changing state, or before going on a break, an agent can use a user code configured to represent break time.

If an agent sets an AUX code using their phone, this is reflected on Avaya Workspaces. If an agent uses Avaya Workspaces to set a user code, this code is also set on Call Center Elite and can be reported on by Call Management System (CMS). In an Avaya Workspaces for Elite solution, agent states and reason codes are always synchronized between agent phones and Avaya Workspaces.

Configure AUX codes for Avaya Workspaces agents using Avaya Control Manager.

Important:

This procedure is mandatory. You must complete this procedure and click Save to ensure the AUX codes are synchronized to UCA. If no AUX codes exist in UCA, agents cannot go Not Ready in Avaya Workspaces.

Before you begin

Ensure that the Avaya Workspaces for Elite clusters are in a running and accepting state.

Procedure

1. Log on to the Avaya Control Manager interface with administrator credentials.
2. On the Avaya Control Manager webpage, click **Communication Manager Objects** > **Aux Reason Code**.

   Avaya Control Manager displays the Communication Manager AUX codes.
3. To add or edit an AUX code, select the **ReasonCode Id** check box.
4. In the **Name** field, type the name for the AUX code.
5. In the **Interruptible** field, type **true** or **false**.
6. Click **Save**.

Adding connectors to the Provisioning Server

Before you begin

Ensure that the Avaya Workspaces for Elite clusters are in a running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Services** > **Provisioning**.
2. On the Provisioning Services List page, perform the following steps:
   a. Select the Provisioning Server.
   b. Click **Edit**.
3. On the Provisioning Services Edit page, perform the following steps:
   a. Select the **Location** tab.
   b. Move the required location from the **Available locations** list to the **Selected locations** list.
   c. Select the **Connectors** tab.
   d. Enable or disable a connector by selecting **Yes** or **No** from the drop-down list.
   e. Click **Save**.

Testing the UCA REST connection

About this task

Use this procedure to test the UCA REST connection.

Note:

By default, UCA requires an authentication token to be supplied in REST request headers. For testing or troubleshooting purposes, you must enable tokenless access by setting the **Enable Tokenless Access** attribute of UCAStoreService to `TRUE`. The change is effective as soon as System Manager replicates the setting to the nodes. After you complete testing or troubleshooting, you must reset this attribute to `FALSE`.

Before you begin

Ensure that the Avaya Workspaces for Elite clusters are in a running and accepting state.

Procedure

Perform one of the following steps to view all Providers:

- In your web browser, enter the following URL:

  `https://<WorkspacesForEliteCluster_IP>/services/UCAStoreService/uca/providers`

- Perform the following steps:

  a. Install a REST client on your Internet browser.

     For example, the Postman application on Chrome.

  b. In the **Get** field, enter the following request URL:

     `https://<WorkspacesForEliteCluster_IP>/services/UCAStoreService/uca/providers`

  c. Click **Send**.

The test returns one of the following results:

- On a newly created system, the test returns an empty JSON block ([ ]).
- On a system with providers configured, the test returns the provider information in JSON format.

Note:

If the test returns a HTTP error, you must investigate and resolve the error.

Configuring a secure connection between Avaya Control Manager and the Avaya Workspaces for Elite server

Obtaining the root certificate from UCA

Procedure

1. In your web browser, enter the following URL:

   `https://<WorkspacesForEliteCluster_IP>/services/UCAStoreService/uca/channels`

   The web browser displays an error on the URL bar to indicate that the connection is not secure.
2. Click on the **Insecure Cert** icon and select the root certificate that the system displays.
3. On the Certification Path tab, click **View Certificate**.
4. On the Details tab, click **Copy to File**.
5. On the Certificate Export Wizard screen, perform the following steps:
   a. Click **Next**.
   b. Select the required format for the certificate and click **Next**.
   c. Browse to the location where you want to export the certificate.
   d. Specify a name for the certificate and click **Next**.
   e. Click **Finish**.

Adding the UCA root certificate to the Trusted Root Certification Authorities list on Avaya Control Manager

Procedure

1. Log on to the server where Avaya Control Manager is installed.
2. Click **Start** > **Run**.
3. In the Run dialog box, type `mmc` and click **OK**.
4. On the Console screen, click **File** > **Add/Remove Snap-in**.
5. On the Add/Remove Snap-in screen, select **Certificates** from the **Available snap-ins** list and click **Add**.
6. On the Certificates Snap-in screen, select **Computer account** and click **Next**.
7. On the Select Computer screen, select **Local computer** and click **Finish**.
8. Click **OK**.
9. On the Console screen, in the left pane, expand **Certificates**.

10. Right-click **Trusted Root Certification Authorities** and click **All Tasks** > **Import**.
11. On the Certificate Import Wizard screen, perform the following steps:
    a. Click **Next**.
    b. Browse to the location where the certificate is placed.
    c. Select the certificate and click **Next**.
    d. Select **Place all certificates in the following store** and click **Next**.
    e. Click **Finish**.

Updating the UCA URL in Avaya Control Manager

About this task

After the root certificate is installed on the Avaya Control Manager server, the UCA URL which is used for the communication between Avaya Control Manager and UCA can be updated to specify https.

Procedure

1. Log on to the Avaya Control Manager interface with administrator credentials.
2. On the Avaya Control Manager webpage, click **Configuration** > **Customer Engagement** > **Workspaces for Elite**.
3. On the Workspaces for Elite Server List page, double-click the Avaya Workspaces for Elite server.
4. On the Workspaces for Elite Server Edit page, in the **API URL** field, update the URL to point to the https endpoint.

Configuring token-based access between Avaya Control Manager and Avaya Workspaces for Elite

About this task

Avaya Workspaces for Elite requires configuration of token-based access to UCA REST APIs. After the configuration has been done, all REST requests must contain a valid token within the request header or the requests are rejected. Token-based access affects Avaya Control Manager management of the Avaya Workspaces for Elite solution and agent logins.

Token enforcement requires that the client of the REST API first requests a token from the Avaya Breeze® platform Authorization Service. The client sends a digitally-signed token request to the service with a list of objects that it wants to access. If the Authorization Service recognizes the client and grants access to the resource, the service returns a signed token. The client uses this token in subsequent calls to the target REST service. The service endpoint checks the validity of the token on each request and processes a request only if the token is valid.

For token-based access to work, perform the following procedures:

- Install signed certificates on the Avaya Control Manager deployment.
- Install the root certificate from the Avaya Breeze® platform cluster hosting the Authorization service as a trusted root certificate authority on the Avaya Control Manager application server.

- Import the Avaya Control Manager public certificate into the Authorization clients list so that the Authorization service recognizes token requests from the Avaya Control Manager server.
- Assign Grants to the Avaya Control Manager client to define the list of resources that can access the Avaya Control Manager server.
- Enable token-based access in Control Manager.
- Configure the Avaya Breeze® platform assigned Client ID for Avaya Control Manager in Avaya Control Manager.

Before you begin

- Ensure that signed certificates are installed on the Avaya Control Manager deployment. For information about certificate installation, see the Avaya Control Manager installation and upgrade documents.
- On the System Manager web console, click **Services** > **Inventory** > **Manage Elements** and identify the root CA that was used to sign the certificate for one of the nodes in the Avaya Breeze® platform cluster that hosts the Authorization service.

Procedure

Create trust between Avaya Control Manager and the Authorization Service

1. Log on to Windows on the Avaya Control Manager server where you must install certificates.
2. Click **Start** > **Run**.
3. In the Run dialog box, type `mmc` and click **OK**.

   The system displays the Microsoft Management Console.
4. Click **File** > **Add/Remove Snap-in**.
5. On the **Add or Remove Snap-ins** window, in **Available snap-ins**, select **Certificates**.
6. Click **Add >**.
7. On the **Certificates snap-in** window, select **Computer account**.
8. Click **Next**.
9. On the **Select Computer** window, select **Local computer**.
10. Click **Finish**.
11. Click **OK**.
12. Expand the **Certificates** folder.
13. Click **Trusted Root Certification Authorities** > **All Tasks** > **Import**.

    The system displays the Certificate Import Wizard Welcome screen.
14. Click **Next**.

    The system displays the File to Import screen.
15. Click **Browse** to locate the root certificate you requested from the CA.

16. Click **Next**.
17. Select **Place all certificates in the following store**.
18. Click **Browse** and select **Trusted Root Certification Authorities**.
19. Click **Next**.
20. Click **Finish**.
21. Try accessing the Authorization URL from a browser using the following URL

    `https://`*`WorkspacesForEliteClusterFQDN`*`:9443/services/AuthorizationService/token`

    Ensure that the link appears as secure in the browser. If you see Error 401, ignore it.

Add the Authorization client to System Manager

22. Log on to System Manager.
23. Navigate to **Elements** > **Avaya Breeze®** > **Configuration** > **Authorization**.
24. On the Authorization Configuration page, click **New**.
25. On the New External Authorization Client page, do the following:
    a. In the **Name** field, enter the name of the Avaya Control Manager server.
    b. In the **Certificate** field, browse to the certificate containing the public key that was exported from the Avaya Control Manager certificate manager.
    c. Click **Commit**.

    The new client now appears in the list of authorized clients.

Add Grants to the Avaya Control Manager application

26. On the Authorization Configuration page, select the Avaya Control Manager client that you added to System Manager.
27. Click **Edit Grants**.
28. On the Edit Grants for Authorization Client page, click **New**.
29. On the Create Grant for Authorization Client page, do the following:
    a. In the **Resource Name** field, select **UCAStoreService**.
    b. In the **Resource Cluster** field, select the Avaya Workspaces for Elite cluster that hosts UCAStoreService.
    c. In the **Feature** field, select **ACM**.
    d. In the **Values** field, select the **delete**, **read**, and **write** check boxes.
30. Click **Commit**.
31. Click **Done**.

32. On the Authorization Configuration page, do the following:
    a. In the **Name** column, locate the entry for the Avaya Control Manager client.
    b. In the **Id** column, locate the ID value for the Avaya Control Manager client and make a note of the ID value.

       You must use the exact ID value when configuring the Avaya Control Manager identity.

Add Grants to the Authorization Service

33. Navigate to **Elements** > **Avaya Breeze®** > **Configuration** > **Authorization**.
34. Select **AuthorizationService** from the list of clients.
35. Click **Edit Grants**.
36. Click **New**.
37. On the Create Grant for Authorization Client page, do the following:
    a. In the **Resource Name** field, select **UCAStoreService**.
    b. In the **Resource Cluster** field, select the Avaya Workspaces for Elite cluster.
    c. In the **Feature** field, select **UserAuthentication**.
    d. In the **Values** field, select the **read** check box.
38. Click **Commit**.
39. Click **Done**.

Configuring the Avaya Control Manager identity

40. Log on to Avaya Control Manager.
41. Navigate to **Configuration** > **Customer Engagement** > **Workspaces for Elite**.
42. Double-click the Avaya Workspaces for Elite server in the list.
43. On the Connection Details tab, do the following:
    a. Select the **Enable Authorization** check box.
    b. In the **Authorization Service URL** field, enter the following value:

       `https://WorkspacesForEliteClusterFQDN:9443/services/AuthorizationService/token`

    c. In the **ACM Instance ID on Breeze** field, enter the ID value of the Avaya Control Manager client that you noted from the Authorization Configuration page in System Manager.
44. Click **Save**.

Enable token enforcement in UCA

45. On System Manager, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.

46. On the Service Clusters tab, do the following:
    a. In the **Cluster** field, select the Avaya Workspaces for Elite cluster.
    b. In the **Service** field, select **UCAStoreService**.
    c. In the **Advanced** group, set the **Enable Tokenless Access** attribute to **FALSE**.
    d. Click **Commit**.

Creating an Avaya Workspaces agent user to handle Elite Voice contacts

About this task

Use this procedure to add an Avaya Workspaces agent user to Avaya Control Manager. This user can log on to Avaya Workspaces as an agent and access the agent features available in Avaya Workspaces.

Before you begin

Ensure that the Avaya Workspaces for Elite clusters are in a running and accepting state.

Procedure

1. Log on to the Avaya Control Manager interface with administrator credentials.
2. On the Avaya Control Manager webpage, click **Users**.
3. On the **Users** tab, click a team, and click **Add**.

   Control Manager displays the User Details page.
4. In the Available applications section, select the **Workspaces for Elite** check box.
5. In the **First Name** field, type the first name for the agent.
6. In the **Surname** field, type the surname for the agent.
7. From the **Profile** list, select **Agent**.
8. In the **LDAP Username** field, type the username used by the Authentication server.

   You must specify the LDAP Username in the email address format. Type the domain name in the second field. This user name is used to log on to Avaya Workspaces.
9. In the **Username** field, type a user name.
10. In the **Password** field, type a password for the user.
11. In the **Confirm password** field, type a password for the user.
12. In the **AVAYA Login** field, enter the Elite agent login ID.

    When creating an agent, if the **Profile** field is set to **Agent** and the **AVAYA Login** field is populated, then this agent is added to Elite.
13. From the **Team** drop-down list, select the team to add this user to.

14. In the **Extension** field, enter the station associated with this agent.

    This is used when logging on to Avaya Workspaces.

    Note:

    You must enter a value in this field.

15. Click **Save**.
16. Select the **Permissions** tab.
17. From the **Role** drop-down list, select **Agent**.
18. Click **Save**.
19. Select the **Skills** tab.
20. From the **Available skills** list select the skills to assign to this user.
21. Click **Save**.
22. Select the **Avaya Oceana** tab.
23. From the **Supervisor** list, select the supervisor for this agent.
24. Select the **Prompt agent for extension number at login** field to display the default extension for the user while logging in, and permit changing the extension.

    This option is useful if Hot Desking is enabled for the user. If this option is not selected, the user is logged in with the default extension.

25. Click **Save**.

Creating an Avaya Workspaces supervisor user

About this task

Use this procedure to add an Avaya Workspaces supervisor user to Avaya Control Manager. This supervisor can log on to Avaya Workspaces as a supervisor and access the supervisor features available in Avaya Workspaces.

Before you begin

Ensure that the Avaya Workspaces for Elite clusters are in a running and accepting state.

Procedure

1. Log on to the Avaya Control Manager interface with administrator credentials.
2. On the Avaya Control Manager webpage, click **Users**.
3. On the **Users** tab, click a team, and click **Add**.

   Control Manager displays the User Details page.

4. In the Available applications section, select the **Workspaces for Elite** check box.
5. In the **First Name** field, type the first name for the supervisor.

6. In the **Surname** field, type the surname for the supervisor.
7. From the **Profile** list, select **Supervisor**.
8. In the **LDAP Username** field, type the username used by the Authentication server.

   You must specify the LDAP Username in the email address format. Type the domain name in the second field. This user name is used to log on to Avaya Workspaces.
9. In the **Username** field, type a user name.
10. In the **Password** field, type a password for the user.
11. In the **Confirm password** field, type a password for the user.
12. In the **AVAYA Login** field, enter the Elite agent login ID.

    When creating a supervisor, if the **Profile** field is set to **Supervisor** and the **AVAYA Login** field is populated, then this supervisor is added to Elite.
13. From the **Team** drop-down list, select the team to add this user to.
14. In the **Extension** field, enter the station associated with this supervisor.

    This is used when logging on to Avaya Workspaces.

    Note:

    You must enter a value in this field.
15. Click **Save**.
16. Select the **Permissions** tab.
17. From the **Role** drop-down list, select **Supervisor**.
18. Click **Save**.
19. Select the **Skills** tab.
20. From the **Available skills** list select the skills to assign to this user.
21. Click **Save**.
22. Select the **Avaya Oceana** tab.
23. Select the **Prompt agent for extension number at login** field to display the default extension for the user while logging in, and permit changing the extension.

    This option is useful if Hot Desking is enabled for the user. If this option is not selected, the user is logged in with the default extension.
24. Click **Save**.

Creating an Avaya Workspaces administrator user

About this task

Use this procedure to add an Avaya Workspaces administrator user to Avaya Control Manager. This user can log on to Avaya Workspaces as an administrator and access the administrative features of Avaya Workspaces.

Before you begin

Ensure that the Avaya Workspaces for Elite clusters are in a running and accepting state.

Procedure

1. Log on to the Avaya Control Manager interface with administrator credentials.
2. On the Avaya Control Manager webpage, click **Users**.
3. On the **Users** tab, click a team, and click **Add**.

   Control Manager displays the User Details page.
4. In the Available applications section, select the **Workspaces for Elite** check box.
5. In the **First Name** field, type the first name for the administrator.
6. In the **Surname** field, type the surname for the administrator.
7. From the **Profile** list, select **Administrator**.
8. In the **LDAP Username** field, type the username used by the Authentication server.

   You must specify the LDAP Username in the email address format. Type the domain name in the second field. This user name is used to log on to Avaya Workspaces.
9. In the **Username** field, type a user name.
10. In the **Password** field, type a password for a user.
11. In the **Confirm password** field, type a password for a user.
12. From the **Team** drop-down list, select the team to add this user to.
13. In the **Extension** field, enter the station associated with this user.

    This is used when logging on to Avaya Workspaces.

    Note:

    You must enter a value in this field.
14. Click **Save**.
15. Select the **Permissions** tab.
16. From the **Role** drop-down list, select **Administrator**.
17. Click **Save**.
18. Select the **Groups to view** tab.

19. Select the check box for the teams and ACM groups that this administrator can view.
20. Click **Save**.
21. Select the **Skills to view** tab.
22. Select the check box for the skills that this administrator can view.
23. Select the **VDNs to view** tab.
24. Select the check box for the VDNs that this administrator can view.
25. Select the **Locations to view** tab.
26. Select the check box for the locations that this administrator can view.
27. Select the **Avaya Oceana** tab.
28. Select the **Prompt agent for extension number at login** field to display the default extension for the user while logging in, and permit changing the extension.

    This option is useful if Hot Desking is enabled for the user. If this option is not selected, the user is logged in with the default extension.
29. Click **Save**.

Configuring screenpops

About this task

Avaya Workspaces provides a screenpop widget to display external web content that can help an agent to complete an interaction. Use Avaya Control Manager to configure screenpops for Avaya Workspaces. You can filter your screenpops by VDN.

Procedure

1. Log on to the Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Workspaces for Elite** > **ScreenPop Configuration**.
3. Click the **ScreenPop** filters tab.
    a. Click **Add**.
    b. In the **Location** field, select the CM location for your solution.
    c. In the **Name** field, type the name of the filter.
    d. In the **Provider** field, select the provider that provides the service.
    e. In the **VDN** field, select the VDN to filter on.
    f. Click **Save**.
4. Click the **Screen Pop Applications** tab.
    a. Click **Add**.

b. In the **Location** field, select the CM location for your solution.

c. In the **Name** field, type the name of the screenpop application.

d. In the **URL** field, type the URL for the screenpop application.

You can add bracket pairs {} to represent additional parameters collected from the contact. For example, an account number entered in a voice response interaction. Add a plus sign (+) between each set of brackets.

Type `http://www.google.com?search={}+{}`.

e. Click **Save**.

5. Click the **Screen Pops** tab.

a. Click **Add**.

b. In the **Location** field, select the CM location for your solution.

c. In the **Name** field, type a name for the screenpop.

Avaya Workspaces displays this name on the screenpop tab.

d. In the **Provider** field, select the provider that hosts the accounts.

For example, select the CM provider.

e. In the **Application Name** field, select the screenpop application previously created.

f. In the **Filter Name** field, select the screenpop filter previously created.

If you do not assign a filter, Avaya Workspaces displays the screenpop for all interactions for the selected provider type.

g. In the **Event** field, select **ACTIVE**.

Avaya Workspaces displays screenpops for the interaction only when the interaction is in the active state.

h. In the **Event Direction** field, select INCOMING or OUTGOING to configure Avaya Workspaces to display the screenpop for incoming or outgoing interactions.

i. In the **Auto Close** field, select **Yes** or **No**.

If you select **Yes**, the screenpop closes when you close the interaction card. If you click **No**, the screenpop remains open after the interaction is closed and you must manually close the screenpop.

j. In the **Launch Internal** field, select **Yes** or **No**.

To display the screenpop in Avaya Workspaces, click **Yes**. To display the screenpop in a new window, click **No**.

k. In the **Priority** field, type the order in which Avaya Workspaces displays the screenpop.

You can configure up to five screenpops for a single interaction. The value in the **Priority** field determines which screenpops to display if more than five screenpops

match the criteria of the contact. The priority value must be unique, or screenpops are overridden.

The **URL** field displays the URL created in the **Screen Pop Applications** tab that is associated with the **Application Name** selected.

l. **(Optional)** In the **Screen Pop Parameters** section, under the **Intrinsics** column, select a parameter.

The **Parameter Position** field displays the number corresponding to the order in which the parameter is added to the URL. The number of parameters depend upon the number of bracket pairs added to the URL.

This step is mandatory if there are placeholders in the application.

To add the originating address as the first parameter for the URL, click the **Originating Address** parameter in the **Intrinsics** column in row 1.

m. Click **Save**.

Configuring CRM integration

About this task

Avaya Workspaces can integrate with Customer Relationship Management (CRM) systems such as SalesForce.

You can administer only one CRM integration.

Procedure

1. Log on to the Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Workspaces for Elite** > **CRM Integration**.
3. Click **Add**.
4. Select a location from the **Location** field.
5. Select the **Enable CRM Integration** check box.
6. In the **CRMIntegrationAppName** field, type the name of the CRM integration.
7. In the **Consumer Key** field, type the consumer key value that identifies this installation to SalesForce.

   In SalesForce, the Consumer Key is known as client_ID.
8. In the **Consumer Secret Key** field, type the secret key value that identifies this installation to SalesForce.

   In SalesForce, this field is known as client_secret.
9. In the **SalesForce Endpoint** field, type the URL of the SalesForce site with which you are integrating Avaya Workspaces.
10. Click **Save**.

Enabling Avaya Breeze® platform authorization on Avaya Aura® Device Services

About this task

The Avaya Workspaces address book uses Avaya Aura® Device Services to search for enterprise directory contacts using LDAP. Use this procedure to enable single sign-on (SSO) capabilities for Avaya Aura® Device Services users that previously authenticated using the Avaya Breeze® platform AuthorizationService. This allows Avaya Workspaces users to use the address book to search for enterprise directory contacts using LDAP, without needing to separately authorize with Avaya Aura® Device Services.

To enable authorization, you must import the Avaya Breeze® platform authorization certificate to Avaya Aura® Device Services. If the certificate is changed, then you must re-upload it to Avaya Aura® Device Services.

For more information about Authorization Service, see *Administering Avaya Breeze® platform*.

Before you begin

Obtain the Avaya Breeze® platform authorization certificate file in the `.PEM` format. For more information, see Deploy Avaya Breeze platform nodes on page 24.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Security Settings** > **Authorization**.
2. Click **Choose File** and select the `.PEM` file that you exported from the Avaya Breeze® platform node.
3. Click **Save**.

Configuring LDAP integration

About this task

The Avaya Workspaces address book uses Avaya Aura® Device Services (AADS) to search for enterprise directory contacts using LDAP. You must set the AADS fully qualified domain name (FQDN) in UnifiedAgentController using the System Manager web console.

AADS queries the Active Directory (AD) global catalogue. All user information fields are not available in the global catalogue by default. Therefore some fields can appear blank in the Avaya Workspaces address book. If you want these missing fields to appear in the address book user profiles, the AD administrator must add these fields to the global catalogue.

Before you begin

- You must install and configure Avaya Aura® Device Services (AADS). For more information, see *Deploying Avaya Aura® Device Services*.
- To retrieve contacts from AADS using LDAP, your solution must include Avaya Aura® 7.1.5 or later.

- Enable cross origin resource sharing (CORS) on AADS. For more information, see *Administering Avaya Aura® Device Services*.
- Ensure that the **active users search filter** and **users search additional filter** in AADS are configured to return users only. For more information, see *Deploying Avaya Aura® Device Services*.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, in the **Cluster** field, select the cluster where UAC is installed.
3. In the **Service** field, select **UnifiedAgentController**.
4. For **AADS FQDN**, select the **Override Default** check box and type the AADS FQDN.
5. Click **Commit**.

Next steps

Verify that Enterprise Directory contacts appear in the address book on Avaya Workspaces.

Support for handling browser close and network connection issues

If an agent closes the browser without logging out or the client session is disconnected, Avaya Workspaces:

- Changes the agent state to Not Ready when the agent is not active on a call.
- Changes the agent state to Not Ready Pending when the agent is active on a call and then changes to Not Ready when the active call ends.
- Sends a pop-up toast message to the supervisor.

The client session can be disconnected due to various reasons, such as browser refresh, browser crash, network changes, system shutdown or sleep, and Avaya Breeze® platform load balancer fail.

When changing the state to Not Ready, Avaya Workspaces also sets the Not Ready reason code. The administrator must configure this reason code in Avaya Control Manager. The agent cannot select this Not Ready Reason code when logged into Avaya Workspaces.

The administrator must also configure the timeout setting to a value from 0 to 300 seconds.

Handling browser close and network connection issues

Procedure

1. Log on to the Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Configuration** > **Customer Engagement**.
3. Click **Workspaces for Elite**.

4. Select the Avaya Workspaces for Elite server and click **Edit**.
5. Click the System Properties tab.
6. Expand the **System Default Codes** section.
7. From the **Browser_Disconnect_Default_Not_Ready_Reasoncode** field, select an AUX code from the available AUX codes.
8. Click **Save**.

Chapter 10: Post-installation verification

Verifying the Avaya Workspaces installation

Before you begin

Configure an Avaya deskphone, Avaya one-X® Agent, or Avaya Agent for Desktop to make calls.

Procedure

1. On a web browser, type one of the following:
   - If security is enabled, `http(s)://`*`WorkspacesForEliteClusterFQDN`*`/services/UnifiedAgentController/workspaces/#/login`.
   - If security is not enabled, `http://`*`WorkspacesForEliteClusterFQDN`*`/services/UnifiedAgentController/workspaces/#/login`.
2. In the **Username** field, type the LDAP user name configured in Avaya Control Manager.
3. In the **Password** field, type the password.
4. Click **SIGN IN**.
5. **(Optional)** In the **Profile** field, select a profile.

   If a station is assigned to the user and you have enabled hotdesking in Avaya Control Manager, you can provide a station number in the **Extension** field. If a voice channel or station is not assigned to the user, the **Profile** field shows **None**.

   Note:

   The field is disabled if the Avaya Workspaces user is already active on another browser and is using hotdesking.
6. Click **ACTIVATE**.

   The system displays the Avaya Workspaces screen.
7. **(Optional)** If the administrator has configured a welcome URL in Avaya Control Manager, Avaya Workspaces displays the welcome widget.
8. Change the state of the user to **Ready**.

   The system queues interactions in the interaction area.
9. Call another user and verify Avaya Workspaces operation.

Chapter 11: Administration

Avaya Workspaces for Elite administration

This section describes how to configure the administrative features of Avaya Workspaces for Elite. You must log on to Avaya Workspaces for Elite as an administrator to access the Admin Settings page.

Avaya Workspaces provides the Widget Framework feature for administrators to:

- Customize the layout and functionality of Avaya Workspaces in a contact center.
- Access Widget APIs to create customized Avaya Workspaces widgets.

For more information about Widget Framework, click the **Overview** button on the Avaya Workspaces administrator interface and see *Widget Framework Developer Documentation*.

Enabling After Contact Work

About this task

Agents enter After Contact Work after completing a call. Use the following procedure if you want the work card to remain visible to agents on Avaya Workspaces during After Contact Work, until the agent dismisses it. This setting applies to all agents.

You configure the length of the After Contact Work interval using CM. For more information about configuring the length of the After Contact Work interval, see Configuring a Hunt Group for Avaya Workspaces for Elite on page 46.

Procedure

1. Log on to Avaya Workspaces as an administrator user.
2. On the Avaya Workspaces administrator interface, click the **Admin Settings** button.
3. Select the **Enable After Contact Work** check box.

Using the Avaya Workspaces compressed layout

About this task

Use the following procedure the enable the compressed layout of the Avaya Workspaces interface. The compressed layout setting applies to all agents. When you enable compressed layout, the workcard area on the Avaya Workspaces interface is minimized, which allows more space for additional widgets.

Avaya recommends only using the compressed layout for voice-only agents.

Procedure

1. Log on to Avaya Workspaces as an administrator user.
2. On the Avaya Workspaces administrator interface, click the **Admin Settings** button.
3. Select the **Use Compressed Layout** check box.

Configuring start work button behavior

About this task

When an agent starts work in Avaya Workspaces, the agent state is set to ready by default. Use the following procedure if you want to allow agents to start work in either the ready or not ready state. This setting applies to all agents.

Procedure

1. Log on to Avaya Workspaces as an administrator user.
2. On the Avaya Workspaces administrator interface, click the **Admin Settings** button.
3. Select the **Allow Agents the choice to Start Work in a Not Ready or a Ready state** check box.

User tokens

When a user logs into Avaya Workspaces, Authorization Service provides the user with a user token. This token always has an expiry time. The minimum expiry time is 1 hour and the maximum expiry time is 24 hours. When this token expires, there is an error toast notification sent to Avaya Workspaces to notify the user that their token has expired. You can enable Avaya Workspaces to send another warning toast notification to the user to warn them that their token will expire within a specified time interval. You can configure this time interval in the UnifiedAgentController svar attributes.

Configuring the time interval for notifying the user of token expiry

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In the **Cluster** field, click **Avaya Oceana® Cluster 2**.
   b. In the **Service** field, click **AgentControllerService**.
3. In the **Advanced Configuration attributes** section, for **Client Session Expiry Interlude**:
   a. Select the **Override Default** check box.
   b. In the **Effective Value** field, enter the time interval in minutes.

      The default time interval is 30 minutes.
4. Click **Commit**.

Chapter 12: Upgrade Avaya Workspaces for Elite

Preupgrade tasks

Adding a third-party root certificate to a cluster

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. Select the cluster, and click **Certificate Management** > **Install Trust Certificate (All Avaya Breeze Instances)**.

   The system displays the Install Trusted Certificate page.
3. Leave the **Select Store Type to install trusted certificate** field set to the default value **All**.
4. Depending on your browser, click one of the following:
   - **Browse**
   - **Choose File**
5. Load the third-party certificate that you want to install.
6. Click **Retrieve Certificate**, and verify whether the details are correct.
7. Click **Commit**.

   The system installs the third-party certificate for all nodes in the cluster.
8. Repeat this procedure for each cluster.

Replacing node identity certificates by a third-party certificate

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. Select a node, and click **More Actions** > **Manage Identity Certificates**.

3. Click the certificate that you want to replace, and click **Replace**.

   For example, click **Security Module HTTPS**.
4. On the Replace Identity Certificate page, click **Import third party certificate**.
5. Depending on your browser, click one of the following:
   - **Choose File**
   - **Browse**
6. Select the third-party identity certificate.
7. In the **Password** field, type a password.
8. Click **Retrieve Certificate**, and verify whether the details are correct.
9. Click **Commit**.

   The system installs and replaces the certificate.
10. Repeat this procedure for each cluster.

Upgrade System Manager and Avaya Control Manager

For information about how to upgrade System Manager and Avaya Control Manager, see *Upgrading Avaya Oceana® Solution*.

Automated upgrade

Automated upgrade overview

This section provides information about the tasks that you must perform before running the automated scripted upgrade of Avaya Workspaces for Elite.

Note:

The automated upgrade procedure does not make any assumptions about your existing deployment. If your current deployment is configured in a manner that does not align with the current documented procedures, the automated upgrade process might fail and you might need to perform a manual upgrade to correct your system.

The high-level tasks of the automated upgrade process are:

- Deleting older loaded versions of the services from System Manager to ensure that System Manager is running only one version of each service.
- Checking the stability of Avaya Breeze® platform nodes.

- Checking the replication status of Avaya Breeze® platform nodes to ensure that none of the nodes is in the audit state.
- Checking the state of services.
- Upgrading Avaya Breeze® platform nodes and the services of Avaya Workspaces for Elite clusters by running the automated script.
- Configuring the Enable Tokenless Access attribute of UCAStoreService.
- Refreshing the certificates on the cluster containing AuthorizationService.

Automated upgrade checklist

Use the following checklist for automated upgrade of Avaya Workspaces for Elite:

No.	Task	Notes	✔
1	Delete older loaded versions of the services from System Manager.	This task ensures that System Manager is running only one version of each service.	
2	Check the stability of Avaya Breeze® platform nodes.	See Checking the stability of Avaya Breeze platform nodes on page 114.	
3	Check the replication status of Avaya Breeze® platform nodes.	See Checking the replication status of Avaya Breeze platform nodes on page 114.	
4	Check the state of the services.	See Checking the state of services on page 114.	
5	Upgrade all Avaya Breeze® platform nodes and the services of Avaya Workspaces for Elite clusters.	See Upgrading Avaya Breeze platform on page 115.	
6	Check the status of services.	Validate if all clusters are in the same state before the migration • If the cluster state before the migration is `Accept`, then the state is set to `Accept` after the migration. • If the cluster state before the migration is `Deny`, then the state is set to `Deny` after the migration.	

Table continues…

No.	Task	Notes	✔
7	Configure the Enable Tokenless Access attribute of UCAStoreService.	Set the **Enable Tokenless Access** attribute of UCAStoreService to `True` to enable requests to access resource end-points without the need of the Authorization token. For more information, see *Deploying Avaya Oceana® Solution*.	
8	Reconfigure the manually backed up snap-in attributes for Avaya Workspaces for Elite.	After configuring these attributes, you must reboot the cluster.	
9	Refresh the certificates on the cluster containing AuthorizationService.	See Refreshing the Authorization Service identity certificates on page 117.	

Checking the stability of Avaya Breeze® platform nodes

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Server Administration**.
2. On the Server Administration page, verify that all Avaya Breeze® platform nodes are in the stable state.

Checking the replication status of Avaya Breeze® platform nodes

Procedure

1. On the System Manager web console, click **Services** > **Replication**.
2. On the Replica Groups page, verify the following:
   - All Avaya Breeze® platform nodes are replicating and are highlighted in green.
   - None of the Avaya Breeze® platform nodes is in the `Audit` state.
   - Validate that the replication status shows a timestamp in the last five minutes. If the timestamp is older, that is, 24 hours, perform a manual replication status check to synchronize the System Manager with all the Avaya Breeze® platform nodes.

Checking the state of services

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.

2. On the Cluster Administration page, in the **Service Install Status** column, verify the check boxes for all clusters to determine that all services in the clusters are in the `Installed` state.

Upgrading Avaya Breeze® platform

About this task

Use this procedure to upgrade the existing Avaya Breeze® platform nodes by running the automated upgrade script.

The automated script does the following:

- Uninstalls the older versions of the services from clusters.
- Deletes services from System Manager.
- Upgrades all Avaya Breeze® platform nodes.
- Loads the latest versions of all services in System Manager.
- Install services to their relevant clusters.

Important:

Ensure that all Avaya Workspaces for Elite nodes are deployed on the same version of VMware ESX.

Before you begin

- Download the `Oceana3610.zip` artifacts file from PLDS.
- Take a snapshot of System Manager.

  You can use the snapshot to recover the previous working state of System Manager. To recover from catastrophic failures, the snapshot is the only recovery mechanism.

  After the successful migration or upgrade, you must remove the snapshot.
- Take a snapshot of the existing Avaya Breeze® platform nodes.

  You can use the snapshot to recover the previous working state of the Avaya Breeze® platform to reattempt the automated or manual upgrade. To recover from catastrophic failures, the snapshot is the only recovery mechanism. For information about how to take a snapshot, see *Upgrading Avaya Breeze® platform*.

  After the successful upgrade and post upgrade testing in production for a limited period of time, you must remove the snapshot.

  Important:

  Avaya recommends that all snapshots must be removed after 48 hours of full production.
- For Avaya Workspaces for Elite upgrades, you must manually take the backup of individual service attributes because they are not saved during the upgrade.

  These attributes need to be manually reconfigured after the upgrade.

Procedure

1. Copy the `Oceana3610.zip` artifacts file to the `/swlibrary` location on System Manager.
2. Log in to the new System Manager virtual machine using an SSH client application, such as PuTTy.
3. Run the following command as a cust user:

   `upgradeSolution /swlibrary/Oceana3610.zip –cg <N> <Configuration Package> <OPTION>`

   In this command:

   - Replace <*N*> with the Cluster Group number of the nodes being upgraded.
   - Replace <*Configuration Package*> with the configuration type to match with the deployment type. For example, WorkspacesForElite-7000.
   - Replace <*OPTION*> with space-separated values depending on the required configuration to include non-mandatory snap-ins.

   The following table list the upgrade script parameters:

Number	Description	Configuration value	OPTION value choices	Sample command
1	Avaya Workspaces for Elite 3.5.x or newer release Voice only with agent sizes up to maximum of 7000 agents	WorkspacesForElite-7000	None	upgradeSolution <*Path To Oceana3610.zip file*> -cg N WorkspacesForElite-7000
2	Avaya Workspaces for Elite 3.5.x or newer release Voice only with agent sizes up to maximum of 2000 agents	WorkspacesForElite-2000	None	upgradeSolution <*Path To Oceana3610.zip file*> -cg N WorkspacesForElite-2000

Important:

- The current version of the command provides validation of these parameters.
- Ensure that you carefully type all option values in the **`upgradeSolution`** command.
- During the upgrade process, the script tries to determine the names of the current clusters and the services installed on the clusters. The script prompts for a confirmation if each cluster name corresponds to a specific cluster.

For example, "Is Cluster 1 name Cluster1_CC (y/n)". If the prompted cluster name is incorrect and you press `n`, the script prompts again until you get the correct cluster name and press `y`.

For these questions, the clusters refer to the naming conventions mentioned in this document.

- You can view the upgrade logs in the `solution-upgrade.log` file in the `/var/log/Avaya` folder on System Manager.

Refreshing the Authorization Service identity certificates

About this task

Use this procedure to refresh the certificates on the cluster containing AuthorizationService. This is a mandatory procedure.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. Select the check box for the cluster containing AuthorizationService.
3. From the **Certificate Management** field, select **Update/Install Identity Certificate (Authorization Service)**.

Manual upgrade

Manual upgrade overview

This section provides information about the tasks that you must perform for manual upgrade of Avaya Workspaces for Elite.

Note:

- This is the standard method of upgrading Avaya Breeze® platform nodes and the services of Avaya Workspaces for Elite clusters if the automated upgrade method is not used.
- If you have already performed a successful automated upgrade, you do not need to do the manual upgrade.

The high-level tasks of the manual upgrade process are:

- Setting the cluster state of all clusters to Denying so that the clusters do not serve any service requests.
- Manually recording the current attributes of all services of Avaya Workspaces for Elite clusters.
- Uninstalling the older versions of all services from clusters so that you can install their latest versions.
- Deleting the older versions of all services from System Manager so that System Manager does not display their older versions.
- Upgrading all Avaya Breeze® platform nodes.
- Loading the latest versions of all services in System Manager.
- Installing all services to their relevant clusters.
- Setting the attributes of the services.
- Setting the cluster state of all clusters to Accepting so that the clusters start serving the service requests.

Manual upgrade checklist

Use the following checklist for manual upgrade of Avaya Workspaces for Elite:

No.	Task	Notes	✔
1	Set the cluster state of all clusters to Denying.	See Setting Cluster State to Denying on page 119.	
2	Manually record the current attributes of all services.	-	
3	Uninstall the older versions of all services from clusters.	See Uninstalling all services from the clusters on page 119.	
4	Delete the older versions of all services from System Manager.	See Deleting all services from System Manager on page 120.	
5	Upgrade all Avaya Breeze® platform nodes.	See Upgrading Avaya Breeze platform nodes using the ISO file on page 120.	
6	Apply the Avaya Breeze® platform patch.	See Applying the Avaya Breeze platform patch on page 121.	
7	Load the latest versions of all services in System Manager.	See Loading SVARs in System Manager on page 62.	
8	Install services to their relevant clusters.	See Installing services to the clusters on page 121.	

Table continues…

No.	Task	Notes	✔
9	Set the attributes of the services.	See Setting cluster services attributes on page 67	
10	Set the cluster state of all clusters to Accepting.	See Setting Cluster State to Accepting on page 122.	

Setting Cluster State to Denying

About this task

Use this procedure to set the cluster state of all clusters to Denying, so that they do not accept any requests.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.

   System Manager displays the Cluster Administration page.
2. Select the check box for Avaya Oceana® Cluster 1.
3. In the **Cluster State** field, select **Deny New Service**.
4. In the Warning: Deny New Service dialog box, click **Continue**.
5. Verify that the Cluster State column for the cluster displays `Denying [x/x]`.
6. Repeat Step 2 to Step 5 for Avaya Oceana® Cluster 2, Avaya Oceana® Cluster 3, Avaya Oceana® Cluster 4, and Provisioning Cluster.

Uninstalling all services from the clusters

About this task

Use this procedure to uninstall the older versions of all services from Avaya Workspaces for Elite clusters.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, select the check box for Elite Cluster 1.
3. Click **Edit**.
4. On the Cluster Editor page, click the **Services** tab.
5. Select the **Uninstall / Force Uninstall** check box for each service, except EventingConnector and CallEventControl.

When you select the check box for a service, you can select the check box for the next service only after a wait period of 10-15 seconds.

6. Click **Commit**.
7. On the Cluster Administration page, select the check box for Elite Cluster 2.
8. Click **Edit**.
9. On the Cluster Editor page, click the **Services** tab.
10. Select the **Uninstall / Force Uninstall** check box for each service, except CallEventControl, EventingConnector, and AuthorizationService.

    When you select the check box for a service, you can select the check box for the next service only after a wait period of 10-15 seconds.
11. Click **Commit**.

Deleting all services from System Manager

About this task

Use this procedure to delete the older versions of all services from System Manager.

Before you begin

Uninstall the older versions of all services from clusters.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. On the Services page, select the check boxes for the services that you want to delete.

   Ensure that the services that you want to delete are in the `Loaded` state.
3. Click **Delete**.
4. In the Delete Service Confirmation dialog box, click **Delete**.

Upgrading Avaya Breeze® platform nodes using the ISO file

About this task

Use this procedure to upgrade the existing Avaya Breeze® platform nodes using the Avaya Breeze® platform ISO file.

Before you begin

Take a snapshot of the existing Avaya Breeze® platform nodes. For more information, see *Upgrading Avaya Breeze® platform*.

After the successful upgrade, you must remove the snapshot.

Procedure

1. Log in to Avaya Breeze® platform nodes using an SSH client application, such as PuTTy.
2. Copy the Avaya Breeze® platform ISO file to each node.
3. Run the following command:

   `upgradeCE <Avaya_Breeze_version_installer>.iso`

   All nodes reboot after the installation is complete.
4. After the reboot, wait until the new nodes replicate successfully with System Manager and pass the maintenance tests.

Applying the Avaya Breeze® platform patch

About this task

Use this procedure to apply the Avaya Breeze® platform patch.

Procedure

1. Log in to Avaya Breeze® platform nodes using an SSH client application, such as PuTTy.
2. Copy the Avaya Breeze® platform patch to each node.
3. Run the following command:

   `patchCE -i <path>/<patch binary>`

   All nodes reboot after the installation is complete.
4. After the reboot, wait until the new nodes replicate successfully with System Manager and pass the maintenance tests.

Installing services to the clusters

About this task

Use this procedure to install the snap-ins to their relevant clusters.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, select the check box for Elite Cluster 1.
3. Click **Edit**.
4. On the Cluster Editor page, click the **Services** tab.
5. In the Available Services list, click the plus sign **(+)** on each service of Elite Cluster 1.

When you click the plus sign **(+)** on a service, System Manager moves the service from the Available Services list to the Assigned Services list. After the service moves to the Assigned Services list, you can click the plus sign **(+)** on the next service.

6. In the Available Services list, click the plus sign **(+)** on the latest versions of the CallEventControl and EventingConnector services.
7. In the Assigned Services list, click **Uninstall** for the older installed versions of CallEventControl and EventingConnector services.
8. Click **Commit**.
9. On the Cluster Administration page, select the check box for Elite Cluster 2.
10. Click **Edit**.
11. On the Cluster Editor page, click the **Services** tab.
12. In the Available Services list, click the plus sign **(+)** on each service of Elite Cluster 2.

    When you click the plus sign **(+)** on a service, System Manager moves the service from the Available Services list to the Assigned Services list. After the service moves to the Assigned Services list, you can click the plus sign **(+)** on the next service.
13. In the Available Services list, click the plus sign **(+)** on the latest versions of the CallEventControl, EventingConnector, and AuthorizationService services.
14. In the Assigned Services list, click **Uninstall** for the older installed versions of CallEventControl, EventingConnector, and AuthorizationService services.
15. Click **Commit**.
16. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
17. On the Services page, verify that the state of all services is `Installing`.

    The state changes to `Installed` when the installation is complete.
18. Wait until all services are installed.
19. Restart the Avaya Breeze® platform nodes of Elite Cluster 1 and Elite Cluster 2.

Setting Cluster State to Accepting

About this task

Use this procedure to set the cluster state of all clusters to Accepting, so that they can accept http or https requests.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.

   System Manager displays the Cluster Administration page.

2. Select the check box for Elite Cluster 1.
3. In the **Cluster State** field, select **Accept New Service**.
4. In the Warning: Accept New Service dialog box, click **Continue**.
5. Verify that the Cluster State column for the cluster displays `Accepting [x/x]`.
6. Repeat Step 2 to Step 5 for Elite Cluster 2.

Chapter 13: Centralized Logging

Centralized Logging

Centralized Logging is a feature that you can use to view the logs for all services installed on Avaya Workspaces for Elite clusters using the Kibana interface. To use this feature, you must install the CentralizedLoggingService and set its attributes. After setting the attributes, you must configure the Avaya Workspaces for Elite clusters for Centralized Logging.

Install the CentralizedLoggingService on Avaya Workspaces for Elite Cluster 1, and configure Avaya Workspaces for Elite Cluster 2 for Centralized Logging.

Configuring Avaya Workspaces for Elite Cluster 2 for Centralized Logging

About this task

Use the following procedure to configure Avaya Workspaces for Elite Cluster 2 for Centralized Logging, so that you can use the Kibana interface to view the logs for the services installed on Avaya Workspaces for Elite Cluster 2.

Before you begin

- To perform this procedure, the cluster must be in a Denying state.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, select the check box for Avaya Workspaces for Elite Cluster 2 and click **Edit**.
3. On the Cluster Editor page, select the **General** tab.
4. In the Cluster Attributes section, perform the following steps:
   a. Select or clear the **Use secure connection for centralized logging** check box based on your requirement.
   b. In the **Centralized logging destination** field, select `Breeze Cluster`.
   c. In the **Breeze cluster as destination for centralized logging** field, select Avaya Workspaces for Elite Cluster 2.
5. Click **Commit**.

The system prompts you to ensure that you restart all Avaya Breeze® platform nodes before placing the cluster into the Accept New Service state.

6. Click **OK**.

Security configuration for Centralized Logging

To securely configure Centralized Logging, you must perform the following steps:

- Configure the WebSphere certificate for each Avaya Breeze® platform node on Avaya Workspaces for Elite Cluster 1.
- Select the **Use secure connection for centralized logging** check box while configuring Avaya Workspaces for Elite Cluster 1 for Centralized Logging.
- Enable **Logstash security** while setting CentralizedLoggingService attributes.

Note:

- If you modify the certificates, you must disable and then enable security on the cluster and the snap-in to use the new certificates.

Logging in to Kibana

About this task

Use this procedure to log in to Kibana to view the Avaya Workspaces for Elite logs. Use the Kibana user name and password that you set during the initial configuration of Centralized Logging.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
2. On the Cluster Administration page, from the **Service URL** list for Avaya Workspaces for Elite Cluster 1, select **Kibana URL**.
3. On the Kibana login page, in the **Username** box, type the Kibana user name.
4. In the **Password** box, type the Kibana password.
5. Click **Log in**.

Creating an index pattern in Kibana

About this task

Use this procedure to create an index pattern in Kibana. You can create index patterns only for the indices for which logs are available.

Procedure

1. Log in to Kibana.
2. Click **Management** > **Index Patterns**.

   Kibana displays the Create index pattern page.
3. In the Define index pattern area, do the following:
   a. In the **Index pattern** field, type the name of the index for which you want to create an index pattern.

      For example, `metricbeat`.

      Kibana displays the list of indices for which logs are available. It activates the **Next step** button only when the specified index name matches an item in the list of indices.
   b. Click **Next step**.
4. In the Configure settings area, do the following:
   a. In the **Time Filter field name** field, click `@timestamp`.
   b. Click **Show advanced options**.
   c. In the **Custom index pattern ID** field, do the following to properly show all visualizations on dashboards:
      - For MetricbeatService, type `metricbeat-*`.
      - For PacketbeatService, type `packetbeat-*`.
   d. Click **Create index pattern**.

Searching logs in Kibana

Procedure

1. Log in to Kibana.
2. In the navigation pane, click **Discover**.
3. In the content pane, click the time picker on the upper-right of the screen.
4. On the Time Range screen, choose the date and time range for which you want to view logs.
5. In the **Available Fields** list, click the **add** button next to a log field to move the field to the **Selected Fields** list.

   Kibana updates the content pane to display the logs with the log field that you moved.
6. In the **Search** field, type the search text in the lucene query syntax and click the **Search** button.

   Kibana highlights the related logs in the content pane.

Viewing statistics on the Metricbeat dashboard

Before you begin

Create an index pattern for Metricbeat.

Procedure

1. Log in to Kibana.
2. In the navigation pane, click **Dashboard**.
3. On the Dashboard page, click **[Metricbeat System] Overview** to view the metrics overview of the servers where MetricbeatService is running.

Viewing statistics on the Packetbeat dashboard

Before you begin

Create an index pattern for Packetbeat.

Procedure

1. Log in to Kibana.
2. In the navigation pane, click **Dashboard**.
3. On the Dashboard page, click **[Packetbeat] HTTP** to view the HTTP requests from the servers where PacketbeatService is running.

Chapter 14: Logging

Logs

Each Avaya Breeze® platform node has a log file for all the SVARs deployed on a cluster. If a cluster has two nodes, examine the log files on both nodes.

The system stores logs for Avaya Workspaces at `/var/log/Avaya/services/Service_Name` for the following services:

- AuthorizationService
- CallEventControl
- EventingConnector
- OceanaMonitorService
- UnifiedAgentContextService
- UnifiedAgentController

Downloading the Avaya Workspaces logs

Procedure

1. Log in to Avaya Workspaces.
2. In the navigation pane, click the ⚙ icon.

   The system displays the Settings widget.
3. Click the **LOGS** tab.
4. Select the time period for which you want to view logs.
5. Click one of the following:
   - **DOWNLOAD**: The system downloads a zip file with the log files for Avaya Workspaces to the Downloads folder in your browser. You can then share or send an email with the logs to your Supervisor or support personnel.
   - **UPLOAD**: The system automatically uploads a zip file with the logs for Avaya Workspaces to a pre-configured central storage location set by your administrator. Note the date and time when you click **UPLOAD**. You must share the date and time of the

upload with your Supervisor or support personnel so that they can identify and retrieve the logs.

Modifying the logging configuration

About this task

Use the Logging Configuration page to change the logging level of an installed server on Avaya Breeze® platform servers or a cluster. You can also clear the logs for an installed service.

The log level for a snap-in does not persist when you:

- Upgrade the Avaya Breeze® platform servers on which you installed the snap-in.
- Reinstall the snap-in.

Procedure

1. On the System Manager web interface, click **Elements** > **Avaya Breeze®** > **Configuration** > **Logging**.
2. On the Logging Configuration page, do the following:
3. In the **Cluster** field, select the cluster to which you want to apply the log level.
4. In the **Server** field, select the server to which you want to apply the log level.
5. In the **Service** field, select the snap-in whose logging level you want to change.
6. In the **Log Level** field, select the logging level of the snap-in that you selected.

   The system displays the clusters and instances where the snap-in is loaded.
7. Click **Set Log Level**.
8. To clear the logs of the selected snap-in, click **Clear Logs**.

Chapter 15: Troubleshooting

Internet Explorer 11 does not display the fonts correctly

Solution

1. Open Internet Explorer 11 on your system.
2. On the menu bar, click **Tools** > **Internet Options**.
3. In the Internet Options dialog box, click the **Security** tab.
4. In the **Select a zone to view or change security settings** section, click **Restricted sites**.
5. In the **Security level for this zone** section, click **Custom level**.

   The system displays the Security Settings — Restricted Sites Zone dialog box.
6. In the **Settings** section, click **Downloads** > **Font download**.
7. Click **Prompt**.
8. Click **OK**.
9. Click **Apply**.

Chapter 16: Resources

Documentation

Title	Use this document to:	Audience
Avaya Workspaces for Elite Solution Description	Learn about the product's key features, capacities, and footprint.	Solution Architects, Sales Engineers, Implementation Engineers
Deploying Avaya Workspaces for Elite	Deploy and administer Avaya Workspaces for Elite.	Administrators
Using Avaya Workspaces for Elite	Use the Avaya Workspaces for Elite browser-based application.	Contact Center Agents
Avaya Workspaces for Elite Disaster Recovery	Learn about Avaya Workspaces for Elite Disaster Recover, and how to configure Disaster Recover for your solution.	Solution Architects, Sales Engineers, Implementation Engineers

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at https://documentation.avaya.com.

Important:

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
  - Type a keyword in the **Search** field.
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

  Navigate to the **My Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add content from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive content that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon (👁).

  Navigate to the **My Content** > **Watch list** menu, and do the following:
  - Set how frequently you want to be notified, starting from every day to every 60 days.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.
- Share a section on social media platforms, such as Facebook, LinkedIn, Twitter, and Google +.
- Send feedback on a section and rate the content.

Note:

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

Training

The following courses are available for Avaya Workspaces for Elite:

Course code	Course title	Delivery Type
Avaya Workspaces		
71050W	Integrating and supporting Avaya Workspaces	WBT
71050T	Avaya Workspaces Integration and Support Online Test	Exam
Avaya Aura® Call Center Elite		
73600V	Implementing Avaya Aura® Call Center Elite	vILT
7391X	Avaya Aura® Call Center Elite Exam	Exam
74600V	Supporting Avaya Aura® Call Center Elite	vILT

Support

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

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Index

A

add
- Communication Manager to Avaya Control Manager ...81
- Communication Manager to the location ... 82
- department ... 85
- Provisioning Server connectors ... 90
- site ... 85
- team ... 85

adding
- administrator ... 100
- agent ... 97
- supervisor ... 98
- third-party root certificate ... 111

adding aux codes
- CM ... 54

adding nodes
- Workspaces for Elite cluster 1 ... 71
- Workspaces for Elite cluster 2 ... 72

add to location
- Workspaces for Elite server ... 87

administering ... 108
administrator tasks ... 108
after contact work
- enabling ... 108

applying
- Avaya Breeze® patch ... 121

assign
- location to Application Server ... 83
- location to Synchronizer Service Server ... 84
- location to UCA Proxy Server ... 83

authentication ... 74
authorization identity certificate ... 75
auto answer
- configuring ... 57

auto-in ... 58
aux codes
- configuring ... 89

Avaya Breeze
- importing identity certificate to AADS ... 104

Avaya support website support ... 133
Avaya Workspaces
- logs ... 128

Avaya Workspaces address book ... 104
Avaya Workspaces for Elite
- deployment process ... 14

Avaya Workspaces for Elite administration ... 108

B

BHCC ... 17
browser close and network connection issues ... 105
browser limitations ... 18

C

capacity ... 17
centralized logging
- configuring cluster 2 ... 124

certificate issue ... 130
certificate issue on IE11 ... 130
certificates
- importing Avaya Breeze authorization certificate ... 104

changes in this release ... 9
checking
- replication status of nodes ... 114
- stability of nodes ... 114

client specifications ... 16
cluster attributes
- settings ... 67

CM aux codes ... 54
CM configuration ... 40
collection
- delete ... 132
- edit name ... 132
- generating PDF ... 132
- sharing content ... 132

commissioning ... 79
communication manager ... 34
Communication Manager logging on ... 41
compressed layout ... 109
configuration and deployment details ... 21
configure
- Agent Login ID ... 53
- Agent Phone-sets ... 54
- Application Enablement Services ... 34, 44
- Direct Agent Calling ... 45
- Hunt Group ... 46
- LDAP server certificates ... 27
- LDAP server integration ... 28
- Route Pattern ... 43
- Signaling Group ... 43
- Trunk Group ... 43
- VDN ... 50
- vector ... 50

configuring
- auto answer ... 57
- aux codes ... 89
- CRM integration ... 103
- screenpops ... 101
- token-based access ... 93
- Workspaces for Elite server ... 88
- Workspaces for Elite token-based access ... 93

connection with CSC ... 39, 75
content
- publishing PDF output ... 132
- searching ... 132

content *(continued)*
sharing ... 132
watching for updates ... 132
create
Communication Manager user ... 79
Workspaces for Elite cluster ... 64, 66
Workspaces for Elite server ... 87
create certificate ... 36
create variables ... 48
CSC communication ... 38

D

deleting
services ... 120
deploy
Avaya Breeze nodes ... 24
Workspaces for Elite cluster ... 60
deployment
prerequisites ... 9
deployment checklist
Avaya Breeze nodes ... 25
disk ... 15
documentation portal ... 132
finding content ... 132
navigation ... 132
document changes ... 9
download CA certificate ... 37
downloading logs ... 128

E

enable
CORS ... 74
end entity ... 36

F

finding content on documentation portal ... 132

H

handling browser close
handling network connections ... 105
hardware ... 15

I

IE11 ... 130
import CA certificate ... 37
import server certificate ... 37
InSite Knowledge Base ... 133
installing
services ... 121

L

LDAP
address book ... 104
licensing requirements ... 19
load
license files ... 62
SVARs ... 62
location
Avaya Workspaces for Elite ... 81
logging configuration ... 129
log in to Avaya Control Manager ... 80
log on
Communication Manager ... 41
logs ... 128

M

manual-in ... 58
maximum accounts ... 17
maximum active users ... 17
memory ... 15
Metricbeat ... 127
My Docs ... 132

N

node identity certificates ... 111

O

operating system ... 16
overview ... 11
automated upgrade ... 112
manual upgrade ... 117

P

Packetbeat ... 127
planning ... 15
POM enhancements ... 10
preconfiguration ... 15

R

refreshing
certificates ... 117
related documentation ... 131
replacing node identity certificates ... 111
root certificate ... 92

S

screenpops
configuring ... 101
searching for content ... 132

setting
Cluster State to Accepting 73, 122
Cluster State to Denying 119
sharing content 132
SSO
Avaya Workspaces 30
start work button
behavior 109
support 133
supported browsers 18
switch connection 34
synchronization 86

T

test
UCA REST connection 91
testing 107
third-party root certificate 111
TLS 74
topology 12
training 133

U

UCA root certificate 92
UCA URL 93
uninstalling
services 119
upgrade checklist
automated 113
manual 118
upgrading
Avaya Breeze® 115
upgrading nodes
Avaya Breeze 120
user token 109
user token expiry notification 110

V

vCPU 15
verify
Avaya Breeze platform deployment 26
host name resolution 61
status of nodes 73
verifying installation 107
view
Oceana Monitor Service 76
viewing
dashboard 127
Virtual resource allocation 20
VMware configuration 21
voice resources 40
vSphere 20

W

watch list 132
Workspaces for Elite cluster
reboot 77