Configuring Avaya Workspaces for Call Center Elite with Avaya WebRTC Connect

Release 3.8.3
Issue 2
February 2024

© 2020-2024, Avaya LLC
All Rights Reserved.

Notice

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

Documentation disclaimer

“Documentation” means information published in varying media which may include product information, subscription or service descriptions, 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. Please refer to your agreement with Avaya 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 the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided 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.

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, 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.

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

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 to comply 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, please contact your Avaya Sales Representative.

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

Contents

Chapter 1: Introduction

Purpose

This document provides information about how to prepare, install, and configure Avaya WebRTC Connect and Remote Worker for Avaya Workspaces for Call Center Elite. Administrators can use this document to configure Avaya WebRTC Connect and Remote Worker for Avaya Workspaces for Call Center Elite at the customer site.

Change history

Issue	Date	Summary of changes
2	Feb 2024	Minor changes across the guide.
1	Jan 2024	Initial issue for Avaya Workspaces for Elite Release 3.8.3.

Chapter 2: Avaya WebRTC Connect Solution

Overview

Avaya Workspaces for Call Center Elite supports WebRTC Connect enabled agents, allowing the agents to handle interactions using their browser, without physical phone or a softphone. Agents can handle voice interactions initiated from the customer web portal, smartphone application, or a PSTN device and video interactions initiated from the customer web portal or a smartphone application.

For WebRTC enabled Voice and Video communication, with Avaya Aura Elite platform, the following components must be installed and configured during deployment:

- Avaya Aura® Device Services (AADS)
- Avaya Aura® Web Gateway (AAWG)
- Avaya Aura® Media Server (AAMS)
- Avaya Session Border Controller (ASBCE)
- Avaya Control Manager (ACM)

Remote Worker

Avaya Workspaces for Call Center Elite supports the remote worker functionality for WebRTC Connect enabled agents. With this functionality, remote agents or supervisors who are physically not located in the contact center infrastructure can access Avaya Workspaces for Call Center Elite applications and perform their tasks.

Chapter 3: Planning and preconfiguration

Overview

This section specifies the interoperability requirements to configure Avaya WebRTC Connect Solution.

You must install and commission the following components. This document assumes that these components are already installed and configured:

Component	Supported release
Avaya Agent for Desktop	The Compatibility Matrix provides compatibility information for the Avaya products that are supported with the various releases of Avaya WebRTC Connect Solution. Access the Compatibility Matrix page at https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml.
Avaya Workplace Client for Windows	
Avaya Aura® Application Enablement Services	
Avaya Aura® Call Center Elite	
Avaya Aura® Communication Manager	
Avaya Aura® Device Services	
Avaya Aura® Session Manager	
Avaya Aura® System Manager	
Avaya Aura® Web Gateway	
Avaya Aura® Media Server	
Avaya Breeze®	
Avaya one-X® Agent	
Avaya Session Border Controller	
Avaya Workspaces for Call Center Elite	
Avaya Control Manager	
G430 Media Gateway	

Network configuration

Network bandwidth guidelines

Note:

The bandwidths mentioned here are for ideal scenarios, that is, for LAN or office worker. For remote worker scenarios, there is additional overhead from factors such as VPN, internet service provider, WAN protocols that may be in use, and also the widgets that are enabled on the Workspace UI. Each customer situation varies, and this must be calculated as per the requirement.

Table 1: Avaya WebRTC Connect 3.8 Voice Bandwidth

WebRTC Connect Voice	Min Bandwidth in Kbps	Max Bandwidth in Kbps
Codec Type - G.711	70 Kbps	100 Kbps
Codec OPUS	70 Kbps	100 Kbps

Note:

You must conduct a proper network assessment, as these network specifications are as per the tests conducted in the laboratory conditions.

Table 2: Avaya WebRTC Connect 3.8 Video Bandwidth

WebRTC Connect Video - Resolutions	Min Bandwidth in Kbps	Max Bandwidth in Kbps
1080p	1792	1792 or higher
720p	1024	1792
480p	640	1024
360p	384	640
240p	256	384
180p	128	256

Capacity specifications

The following table shows the Avaya WebRTC Connect capacity specifications.

Customer	Agent	Number of concurrent calls
WebRTC Voice	WebRTC Voice	1000
WebRTC Video	WebRTC Video	500

Supported browser and OS versions

The following table lists the supported browser and operating system (OS) versions for WebRTC Connect Customer Reference Client:

Platform	Version
Android	10.x
iOS	12.x and 13.x
JavaScript	Google Chrome 87, 86, and 85 Firefox 83, 82, and 81 Chromium 87

Chapter 4: Security considerations

Overview

Avaya WebRTC Connect comprises of two layers:

- The core layer where the entire Avaya Aura solution is present, in the private or premise data center.
- The public layer consisting the external and internal firewall and Avaya SBC, depending on whether the agent is remotely located or enterprise agents.

Avaya Aura® Web Gateway connects the public layer to the core layer. You can make calls using Avaya provided mobile WebRTC SDK or application hosted on the web server through public internet. All the calls are routed through Avaya SBCs using HTTPS signaling and media through DTLS-SRTP. When an agent is a remote worker, logging in through public internet, the signaling goes through Avaya SBC and internal firewall over secure connection.

Table 3: Secure connections between various components

Connection	Protocol	Layer
Customer Web Browser	HTTPS	Public
Customer Mobile phone	HTTPS	
External/Internal SBC - AAWG	SIP/HTTPS	
AAWG-AADS	TLS	Core
AAWG-LDAP	LDAP-S	
AAWG-SMGR	Enrollment	
AAWG-AAMS	TLS	
AAWG-SM	TLS	

Table 4: Media Security

Incoming Call Type	Security Type	Algorithm
Browser based SDK-SBC-AAWG-AAMS-CM-AMS-Workspace Agent	DTLS-SRTP	SRTP using the below algorithm AES_CM_128_HMAC_SHA1_80 AES_CM_128_HMAC_SHA1_32

Table continues…

Incoming Call Type	Security Type	Algorithm
Mobile Client SDK-SBC-AAWG-AAMS-CM-AMS-Workspace Agent	DTLS-SRTP	SRTP using the below algorithm AES_CM_128_HMAC_SHA1_80 AES_CM_128_HMAC_SHA1_32
PSTN Call	SRTP	Secure after Avaya SBC using the below algorithms AES_CM_128_HMAC_SHA1_80 AES_CM_128_HMAC_SHA1_32

Port Matrix

For information on port matrix, see *Avaya Port Matrix Avaya WebRTC Connect 4.0 (Remote Worker)*.

Secure Communications using Transport Layer Security

Transport Layer Security (TLS) is a cryptographic protocol used to increase security over computer networks. The solution supports TLS 1.0 and TLS 1.2. When you deploy the solution, by default, TLS 1.0 is configured. The highest supported TLS version is 1.2.

You can change the TLS versions by using the following options:

- Globally from Avaya Aura® System Manager
- Through the Cluster Editor page in the System Manager

Setting TLS is a security requirement for internal communications, and external communications with databases and LDAP.

Certificate requirement checklist

The following are the security considerations regarding certificates:

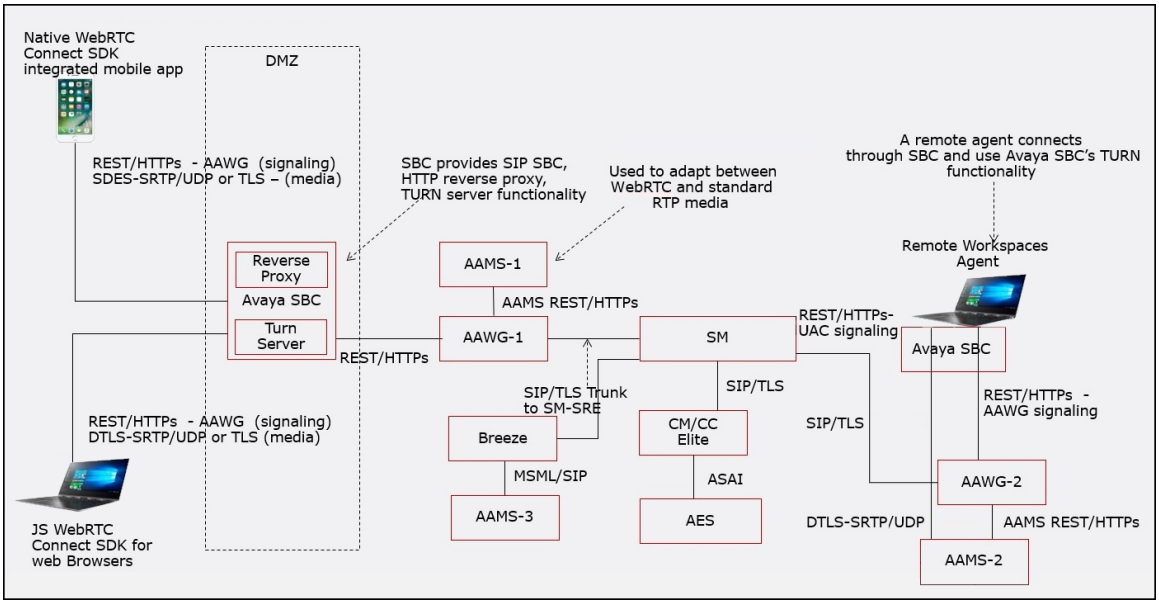
No.	Task	Description	✔
1	Replace the default certificate on all Breeze nodes.	Creating the common certificate on page 26	

Table continues…

No.	Task	Description	✔
2	Create certificates for SBC (Client and Server)	• Creating the common server certificate on page 76 • Creating the common client certificate on page 75	
3	Importing Breeze common certificate on AAWG ad AADS Authorization	• Importing the authorization certificate on page 27 • Enabling authorization on Avaya Aura® Web Gateway on page 53 • Enabling Avaya Breeze platform authorization on Avaya Aura Device Services on page 33	

Security Overview

The core applications of the solution must be secured at the core level, followed by the clients and applications, which connect securely to the inner core, and then the security at the entire enterprise level in the internet zone and beyond.



Note:

Only the key media and call signaling related components are displayed in the diagram.

The inner layer of the solution contains the core applications, Avaya Aura® Core and Avaya Workspaces for Call Center Elite applications. The solution is secured by enabling the security between all the core applications. The applications outside of the core interact with the core applications. Security must be enabled for all communications and data exchange between these two layers. The applications and clients on the internet must access the contact center functionality in a secure and reliable manner.

This chapter describes the types of configurations, settings, and the techniques that the customer can use to secure all the areas, starting at the core, to the internet zone at the edge of company networks.

Core Applications Security

The operations require the three core applications to communicate with each other. Avaya Workspaces for Call Center Elite uses the Avaya Aura® Suite of applications comprising Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Application Enablement Services, and Avaya Aura® Media Server to provide the voice platform for PSTN voice contacts.

You can secure communications and data transfer for the core applications using:

- Secure Communications with https and wss (web socket secure)
- Token Based Authorization
- TLS 1.2
- FQDNs
- A root CA certificate in conjunction with Identity Certificates to deliver a Server Authentication Model

Avaya Workspaces for Call Center Elite core applications are primarily Avaya Breeze® platform-based software applications called snap-ins or services. The software applications take the configuration data from configurable parameters called Attributes.

The following are examples of snap-in attributes related to security, which can be set on the Elite Configuration Service, and automatically applied to all other Avaya Workspaces for Call Center Elite services:

- Secure Connections to Database - Default Value = True
- Toggle Secure Mode - Default Value = False (https on by default)
- Enable Tokenless Access - Default Value= False (Token required by default). All REST requests for these interfaces must contain a valid token within the request header or they are rejected.
- TLS version - Default Value = 1.2
- Enable Secure Communications - Default Value = True
- Authorization Required to Contact Service - Default Value = True
- Authorization Required for Service - Default Value = True

For all these attributes except the **Enable Tokenless Access** attribute, a value of `True` specifies that the web communications into these snap-ins are secure and also use token-

based authorization. However, for enhanced security, Avaya recommends that all customers use the combination of Fully Qualified Domain Name (FQDN) and Domain Name Server (DNS) in conjunction with security certificates for all interfaces accessible in the solution. Avaya Workspaces for Call Center Elite Breeze Clusters must use an FQDN. After you configure all applications in the solution for security, all clients and applications can securely communicate with Avaya Workspaces for Call Center Elite .

Certificate Authority (CA)

A Certificate Authority (CA) is a trusted entity that issues digital certificates and public-private key pairs. A CA verifies the identity of an individual or organization before issuing a digital certificate. A CA can be an external (public) or internal (private) entity configured inside an enterprise network. A Certificate Authority is a critical security service in a network.

Every Avaya Workspaces for Call Center Elite deployment has an Avaya Aura® System Manager deployed, and one of its functions is that of a CA. You can use System Manager's CA to secure the communications between the Avaya Aura® components, Avaya Workspaces for Call Center Elite, Avaya Breeze® platform components, and all the other surrounding components in the solution.

Customers can implement a solution with their own Enterprise CA, either replacing System Manager as the CA or using it as a sub CA. Before attempting to make certificate changes in the deployed solution, you must have a solution level view to understand which network elements are affected. This requires planning and network audits before deploying new certificates.

A certificate change goes through the following four stages:

- Assessment: Identify and scope the migration work for your network.
- Planning: Plan and schedule the migration tasks.
- Migration: The actual migration which includes software upgrades, Trust Certificates deployment, and Identity Certificate deployment.
- Post-migration: Ongoing audits to avoid certificate expiration.

For public or private CA, the procedures for enabling security and applying the required certificates are almost identical. If you are using a third-party public CA, a third-party vendor certificates require time to be made available and the customer to work with the third-party to obtain the certificates after the correct information about their system is provided.

Using System Manager as a Root CA means the end customer can perform the certificate creation process themselves. For more details on System Manager as a CA, see the Avaya Aura® System Manager documentation suite.

Chapter 5: Configure Avaya Workspaces for Call Center Elite Solution with Avaya WebRTC Connect agents

Avaya WebRTC Connect solution configurations and prerequisites

Configurations

Avaya Workspaces for Call Center Elite provides the following WebRTC Connect configurations. Based on your requirements, you can choose from the following configurations and complete all tasks:

- Avaya Workspaces for Call Center Elite with WebRTC Connect agents.

  With this configuration, WebRTC Connect agents can answer PSTN voice calls.

- Avaya Workspaces for Call Center Elite with web and mobile voice calls.

  With this configuration, phone-enabled agents can answer web and mobile voice calls that customers make through web and mobile devices on the public internet.

- Avaya Workspaces for Call Center Elite with web and mobile voice calls and WebRTC Connect agents.

  With this configuration, WebRTC Connect and phone-enabled agents can answer PSTN, web, and mobile voice calls.

- Avaya Workspaces for Call Center Elite with web and mobile video calls and WebRTC Connect agents.

  With this configuration, WebRTC Connect agents can answer web and mobile video calls.

Important:

- Before proceding with any of these configurations, you must deploy the Elite voice solution.
- WebRTC Connect agents do not support the Auto answer feature. Therefore, do not configure WebRTC Connect agents to use this feature.
- Avaya Workspaces for Call Center Elite supports web and mobile video calls only if you have Avaya Workspaces for Call Center Elite 7.1.3 or later.

- Hot Desking configuration does not apply to WebRTC Connect agents.
- Web calls made using the Microsoft Edge browser do not support STUN, TURN-TCP, or TURN-TLS.
- Web calls made using the Microsoft Edge browser support UDP TURN.
- WebRTC Connect only supports secure deployment options.

Prerequisites

The following are the prerequisites for the WebRTC Connect solution:

- Network Time Protocol (NTP) server configured
- Fully Qualified Domain Name (FQDN) configured on the DNS server
- LDAP/Active Directory
- Avaya Aura® Communication Manager, Avaya Aura® Session Manager, Avaya Aura® System Manager, and Avaya Breeze® platform.
- Avaya Aura® Media Server for Avaya Aura® Web Gateway
- Avaya Aura® Device Services
- Avaya Aura® Web Gateway
- Avaya Control Manager 9.0.1 and higher
- Avaya Contact Recorder Advanced for recording

Configuration checklist

Use the following checklist to configure Avaya Workspaces for Call Center Elite with WebRTC Connect agents so that WebRTC Connect agents can answer PSTN voice calls.

Before you proceed with the tasks listed in the checklist, ensure the following:

- Avaya Aura® Call Center Elite 7.1.3 or higher is deployed and configured. Minimum version supported for Application Enablement Services is 8.1 or higher. See *Avaya Aura® Call Center Elite Solution*.
- The basic voice and video calls are functional for SIP and H.323 users.
- Complete each step in the checklist before proceeding to the next step.

No.	Task	Description	✔
1	Configure LDAP	See Configure LDAP on page 23.	

Table continues…

No.	Task	Description	✔
2	Synchronize LDAP users in System Manager	See Synchronizing LDAP users in System Manager on page 24.	
3	Assign SIP Handles to the synchronized LDAP users in System Manager	-	
4	Install and configure Avaya Aura® Device Services, Avaya Aura® Media Server, and Avaya Aura® Web Gateway.	See the following: • Avaya Aura Device Services deployment on page 29. • Avaya Aura Media Server deployment on page 35. • Avaya Aura Web Gateway deployment and configuration on page 46.	
5	Publish the COMM_ADDR_HANDLE values of the WebRTC agent on Avaya Aura® Device Services	See Publishing COMM_ADDR_HANDLE values on Avaya Aura Device Services on page 34.	
6	Configure the voice media path	See the following:. • Configuring codecs in Avaya Aura Web Gateway on page 53. • Prioritizing codecs in Avaya Aura Media Server on page 54. • Prioritizing codecs in Communication Manager on page 54.	
7	Configure authorization on Avaya Aura® Web Gateway	See Avaya Aura Web Gateway authorization on page 52.	
8	Create WebRTC agents that can use media in browsers	See Creating a user in Avaya Control Manager on page 62.	

Table continues…

No.	Task	Description	✔
9	Ensure that the agent is able to log on to Avaya Workspaces	See Logging in to Avaya Workspaces on page 63.	

Configure LDAP

The LDAP configuration involves the following:

- Preconfiguration
- Create a user in Active Directory
- Synchronize the LDAP users in Avaya Aura® System Manager

LDAP Preconfiguration

Ensure that you install and configure Windows Active Directory or any supported LDAP and also configure System Manager with LDAP by using a secure link.

- Get a working LDAP to complete the installation of Avaya Aura® Device Services and Avaya Aura® Web Gateway.
- Assign a user to the selected admin group to administer the system after the installation.
- Create the following in your AD or LDAP system:
  - A domain for the users.

    This domain does not need to match the SIP domain. Multiple Avaya Workspaces for Call Center Elite deployments can use the same users from the same LDAP or domain.
  - An organizational unit under the domain.
  - A test user that Avaya Aura® Device Services uses for connectivity.
  - Two LDAP security groups for authenticating users and administrators.

    The following table lists the groups:

Group name	Purpose
AADS_User	General users including all Avaya WebRTC Connect users and Avaya Aura® Device Services users.
AADS_Admin	Users who can administer Avaya Aura® Device Services and Avaya Aura® Web Gateway after logging on to the AD or LDAP system.

Creating a user in Active Directory

About this task

Use this procedure to create a user in Active Directory who can act as a general user for Avaya Aura® Device Services, and can also administer Avaya Aura® Device Services and Avaya Aura® Web Gateway.

Procedure

1. Log in to the server containing the Active Directory.
2. Click **Start** > **Administrative Tools** > **Active Directory Users and Computers**.
3. In the navigation pane, expand the domain that you created for the users.
4. Right-click the Active Directory organizational unit (OU) and click **New** > **User**.
5. In the **New Object - User** dialog box, in the **First name** field, enter the first name of the user.
6. In the **Last name** field, enter the surname of the user.
7. In the **User logon name** field, enter the user name.
8. Click **Next**.
9. In the **Password** field, enter a password for the user.
10. In the **Confirm Password** field, re-enter the password.
11. Clear the **User must change password at next logon** check box.
12. Select the **Password never expires** check box.
13. Click **Next**.
14. Click **Finish**.

    The server displays the new user in the list in the content pane.
15. In the content pane, right-click the new user and click **Add to a group**.
16. In the Select Groups dialog box, add the user to the standard users group and the appropriate administrator group, and click **OK**.

    For more information, see LDAP Preconfiguration on page 23.

Synchronizing LDAP users in System Manager

About this task

Use this procedure to synchronize LDAP users in System Manager.

Procedure

1. On the System Manager web console, click **Users** > **Directory Synchronization** > **Sync Users**.
2. On the User Synchronization page, on the Synchronization Datasources tab, click **New**.

The New User Synchronization Datasource page opens.

3. In the Directory Parameters section, in the **Datasource Name** field, enter the name to identify Active Directory.
4. In the **Host** field, enter the FQDN address of your LDAP server.

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

   For example, myDomain\Administrator.
6. In the **Password** field, enter the password for the LDAP login account that you specify.
7. In the **Port** field, enter the port number as `636`.
8. In the **Base Distinguished Name** field, enter the LDAP details.

   For example, CN=myDomain.com,DC=myDomain,DC=com
9. In the **Search Filter** field, enter the LDAP search string.

   For example, CN=Alex*.
10. Select the **Use SSL** check box.
11. Click **Test Connection**.
12. In the Attribute Parameters section, click **Add Mapping** to add a row.
13. From the drop-down list on the left, select **cn**.
14. From the corresponding drop-down list on the right, select **sourceUserKey**.
15. Click **Add Mapping** to add another row.
16. From the drop-down list on the left, select **mail**.
17. From the corresponding drop-down list on the right, select **loginName**.

    Note:

    Instead of the **mail** field pointing to **loginName**, you can also use **userPrincipalName** depending on the configuration of the LDAP server. For example, if the **mail** field is not set in the LDAP server.
18. Click **Add Mapping** to add another row.
19. From the drop-down list on the left, select **givenName**.
20. From the corresponding drop-down list on the right, select **surname**.
21. Click **Add Mapping** to add another row.
22. From the drop-down list on the left, select **givenName**.
23. From the corresponding drop-down list on the right, select **givenName**.
24. Click **Add Mapping** to add another row.
25. From the drop-down list on the left, select **givenName**.

26. From the corresponding drop-down list on the right, select **displayName**.
27. Click **Save**.
28. On the User Synchronization page, click **Active Synchronization Jobs**.
29. Click **Create New Job**.
30. 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.
31. On the User Synchronization page, click **Synchronization Job History**.
32. In the **Status** column, verify that the status of the job is `RUNNING`.

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

Creating the common certificate

About this task

If your system uses authorization certificates created by a third-party certificate authority, you may reuse them. Alternatively, you can create authorization certificates using the same service. You can reuse the existing certificates if they are created with the FQDNs and IP addresses of every node in the cluster.

Important:

Authorization certificates are used only for internal communication. Therefore, you can use the System Manager-generated certificates. If you already have a valid `pk12`-format certificate file, you can skip these steps.

Procedure

1. **Create an end entity**: Log on to Avaya Aura® System Manager.
2. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
3. In the navigation pane, in the RA Functions section, click **Add End Entity**.
4. In the **End Entity Profile** field, select `INBOUND_OUTBOUND_TLS`.
5. In the **Username** field, enter a user name.
6. 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.
7. In the **Confirm Password** field, re-enter the password.

8. In the **CN, Common name** field, enter the FQDN of the cluster that AuthorizationService is installed on.
9. In the first **DNS Name** field, enter the Security Module FQDN for one of the nodes of the cluster.
10. In the second **DNS Name** field, enter the Security Module FQDN for the second node of the cluster.

    In a small solution, AuthorizationService is installed on Avaya Workspaces for Call Center Elite Cluster 1 that contains three nodes. Therefore, you must also configure the **DNS Name** field for the third node of the cluster.
11. In the **IP Address** field, enter the IP address of the cluster.
12. In the **Token** field, select `P12 file`.
13. Click **Add**.
14. **Create a keystore**: On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
15. In the navigation pane, click **Public Web**.
16. On the EJBCA welcome page, in the navigation pane, click **Create Keystore**.
17. On the Keystore Enrollment page, enter the user name and password that you specified while creating the end entity.
18. Click **OK**.
19. Select the **Key Length** as 2048 bits.
20. Click **Enroll**.
21. Save the certificate file.

Importing the authorization 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 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, select the **Import third party certificate** option.
5. In the **Please select a file (PKCS#12 format)** field, browse and select the P12 file that you generate.
6. In the **Password** field, enter the password that you specified while creating the end entity.
7. Click **Commit**.

8. Repeat Step 2 to Step 7 for the other nodes of the cluster.
9. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
10. Select the cluster that contains AuthorizationService.
11. Click **Certificate Management** > **Update/Install Identity Certificate (Authorization Service)**.

    System Manager displays a message stating that the certificate has been updated successfully.
12. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Configuration** > **Authorization**.
13. On the Authorization Configuration page, on the Clients tab, select **UnifiedAgentController**.
14. Click **Edit Grants**.
15. On the Edit Grants for Authorization Client page, click **New**.
16. In the **Resource Name** field, select **UnifiedAgentController**.
17. In the **Resource Cluster** field, select the cluster that contains UAC.
18. In the **Feature** field, select **desktop**.
19. Select the check box for **access**.
20. Click **Commit**.
21. Click **Done**.

Exporting the Avaya Breeze® platform Authorization Identity Certificate

About this task

Requests from clients to the Avaya Aura® Web Gateway server involves passing an authorization token in the request. The authorization is handled through Avaya Workspaces for Call Center Elite cluster 2 that hosts the *AuthorizationService* snapin. Avaya Aura® Web Gateway is a third-party server. Therefore, you must configure the Avaya Breeze® platform Authorization Certificate on Avaya Aura® Web Gateway.

An issue arises because 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 are rejected. To enable authorization on Avaya Aura® Web Gateway, you must first replace the Authorization Identity Certificate on each Avaya Breeze® platform node with a single System Manager generated identity certificate. Import this identity certificate into your Avaya Aura® Web Gateway.

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.

Avaya Aura® Device Services deployment

Avaya Workspaces for Call Center Elite requires Avaya Aura® Device Services to provide login services to Video-enabled SIP agents through a browser endpoint.

Installing Avaya Aura® Device Services

About this task

Use this procedure to install Avaya Aura® Device Services.

Before you begin

On the System Manager web console, click **Elements** > **Session Manager** > **Dashboard** and verify that all Session Manager instances are up and running.

Procedure

1. Log on to AADS terminal.
2. Go to the Avaya directory by typing the following command:

   `cd /opt/Avaya`

3. Run the following command:

   `app install`

   The Initial Installation Configuration screen appears.

4. Select the **Cluster Configuration** menu and ensure that the **Initial cluster node** option is set to `y`.
5. To return to the previous menu, select **Return to Main Menu** and press **Enter**.
6. Select the **Front-end host, System Manager and Certificate Configuration** menu and configure the settings that are accessible from the menu.
7. In the **Front-end FQDN** field, type the Avaya Aura® Device Services FQDN to extend the system to an Avaya Aura® Device Services cluster.

You must use the hostname corresponding to the virtual IP address. For a standalone Avaya Aura® Device Services, this field is the same as the local front end host.

8. In the fields specific to System Manager, enter the required values.

   Keystore password must have six or more characters. The password must be the same on all nodes in the cluster.

   After you enter the System Manager FQDN and press **OK**, the installer tries to check the validity of the hostname.

9. Select **Return to Main Menu** and press **Enter**.
10. Select the **Session Manager Cassandra Configuration** menu and type the Session Manager Management and Asset IP addresses.
11. Read the End User License Agreement (EULA) and press **Accept** to accept the EULA.

    The system configures the other settings such as required RPMs, downloads certificates from System Manager, creates database schema, and does the required initial configuration required for the Avaya Aura® Device Services server installation.

12. Select **Continue** to finish the installation.
13. Select **LDAP Configuration**.
14. On the LDAP configuration screen, type values for each parameter manually.

    Important:

    Do not copy-paste these values to avoid invalid characters such as spaces.

15. Navigate to **Advanced LDAP parameters** and click **Select**.

    Note:

    Ensure that you use the same groups for **User Role** and **Administrator Role** created on LDAP. See LDAP Preconfiguration on page 23.

16. On the Advanced LDAP parameter screen, verify the default values for the parameters and update the required values.
17. Select **Return to Main Menu** and press **Enter**.
18. Navigate to **TestUser** and click **Select**.
19. Add an LDAP test user for better validation of the LDAP parameters.

    The test user must be a valid user on LDAP and must be present in the provided Base Context DN. The LDAP user must correspond to **UID Attribute ID**.

20. Click **OK**.
21. Click **Apply**.
22. Click **Yes**.
23. Click **Continue**.

24. Leave the **CORS Configuration** and **Serviceability Agent Configuration** fields unchanged.
25. Click **Continue**.
26. On the prompt to restart Avaya Aura® Device Services, click **Yes**.
27. Click **Continue**.

Adding a data center

About this task

Use this procedure to add a data center in System Manager.

Procedure

1. On the System Manager web console, click **Elements** > **Session Manager** > **Session Manager Administration** > **Groups**.
2. On the Groups page, click the **Session Manager Groups** tab.
3. Click **New** > **New data Center**.
4. In the **Name** field, enter a name for the data center.
5. In the **Description** field, enter the description of the data center.
6. Click **Commit**.

Assigning Session Manager to the data center

About this task

Use this procedure to assign Session Manager to the newly created data center.

Procedure

1. On the System Manager web console, click **Elements** > **Session Manager** > **Session Manager Administration** > **Groups**.
2. On the Session Manager Groups tab, select a data center and click **Edit**.

   The system displays the Edit Session Manager Group page.
3. To assign Session Manager to a data center, under the **SMs unassigned or assigned to other Data Center** section, select the data center name from the Data Center list.

- If you select the same data center name for Session Manager, System Manager refreshes the page and displays the assigned data center under the SMs in Data Center section.
- If you select another data center name for Session Manager, System Manager displays the assigned data center under the **SMs unassigned or assigned to other Data Center** section.

4. Click **Commit**.

   The system displays the Confirm Data Center assignments page.

5. Verify the data center and Session Manager assignment.
6. Click **Confirm**.

Adding an Avaya Aura® Device Services instance to System Manager inventory

About this task

Use this procedure to add an instance of Avaya Aura® Device Services to System Manager inventory.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, click **New**.

   System Manager displays the New Elements page.
3. In the **Type** field, select `Avaya Aura Device Services`.

   System Manager displays the New Avaya Aura Device Services page.
4. On the General tab, in the **Name** field, enter the name of the Avaya Aura® Device Services server.
5. In the **Node** field, enter the IP address of the Avaya Aura® Device Services server.
6. In the **Description** field, enter the description of the Avaya Aura® Device Services server.
7. Click the **Attributes** tab.
8. On the Attributes tab, in the **Login** field, enter the user name to access the Avaya Aura® Device Services server.

   The user name that you enter in this field is the administrator user name provided during the Avaya Aura® Device Services OVA deployment.
9. In the **Password** field, enter the password to access the Avaya Aura® Device Services server.

   This is the administrator password provided during the Avaya Aura® Device Services OVA deployment.
10. In the **Confirm Password** field, re-enter the password to access the Avaya Aura® Device Services server.
11. In the **Version** field, enter the Avaya Aura® Device Services base version (7).
12. In the **Location** field, enter the location of the Avaya Aura® Device Services server.

    This is an optional field.
13. Click the **General** tab.
14. Select the TrustManagement access profile and click **Edit**.
15. Leave the **Container type** field blank.

16. In the **Host** field, enter the hostname of the Avaya Aura® Device Services server.
17. Click **Save**.
18. To add an EMURL access profile to enable SSO login, on the General tab, in the Access Profile area, click **New**.
19. In the **Access Profile Type** field, select `EMURL`.
20. In the **Host** field, enter the FQDN of the Avaya Aura® Device Services server.
21. In the **Port** field, type `8445`.
22. In the **Path** field, type `/admin`.
23. Click **Save**.
24. Click **Commit**.

Pairing Session Manager with an Avaya Aura® Device Services server

About this task

Use this procedure to pair Session Manager with an Avaya Aura® Device Services server.

Procedure

1. On the System Manager web console, click **Elements** > **Session Manager** > **Session Manager Administration** > **Session Manager Administration**.
2. On the Session Manager tab, select an instance and click **Edit**.

   System Manager displays the Edit Session Manager page.
3. In the **Avaya Aura Device Services Server Pairing** field, select an Avaya Aura® Device Services server to pair with Session Manager.
4. Click **Commit**.

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 information about how to create the common certificate, import it in Avaya Breeze® platform nodes, and export the Avaya Breeze® platform authorization Identity Certificate see:

- Creating the common certificate on page 26
- Importing the authorization certificate on page 27
- Exporting the Avaya Breeze platform Authorization Identity Certificate on page 28

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**.

Publishing COMM_ADDR_HANDLE values on Avaya Aura® Device Services

Procedure

1. On the Avaya Aura® Device Services web administration portal, click **Dynamic Configuration** > **Configuration**.
2. On the Configuration page, click the **Group** tab.
3. In the **COMM_ADDR_HANDLE_TYPE** field, click `Avaya SIP`.
4. In the **COMM_ADDR_HANDLE_LENGTH** field, enter the number of digits in the extension number of the SIP agent.
5. Click **Publish**.

   The portal displays the Publish/Delete Settings dialog box.
6. Select the **Group settings will be applied to group** check box.
7. In the text box, type the first five characters of the LDAP group that contains the agents.

   For example, AADS_User.
8. In the drop-down list, click the group.
9. Click **Publish**.
10. Click **Yes**.
11. To verify whether the values are published, in your web browser, enter the following URL:

    `https://<Avaya Aura Device Services FQDN>:8443/acs/resources/configurations`

12. On the prompt, enter the login credentials of the LDAP user who is a part of the LDAP user group.
13. Verify the output.

    The following is an example of the output:

```
## File Generation Notes
## Avaya Dynamic Configuration Service does not recognize User-Agent - Mozilla/5.0 (Windows)

SET SIPSECURE 0
SET SIPENABLED 1
SET SIPDOMAIN oceana.com
SET SIPUSERNAME 8831093
SET SIPHA1 70e9ab3f778a27d0012d725f941783c8
SET ACSPORT 8843
SET ACSSECURE 1
SET ACSENABLED 1
SET ACSSSO 1
SET SIP_CONTROLLER_LIST 10.133.34.202:5061;transport=TLS
SET ACSSRVR 10.133.34.204
SET SIPPROXYSRVR 10.133.34.202
SET SIPPORT 5061
SET LOCKED_PREFERENCES "SIPSECURE,SIPENABLED,SIPDOMAIN,SIPUSERNAME,SIPHA1,ACSPORT,ACSSECURE
SET OBSCURE_PREFERENCES ""
```

Avaya Aura® Media Server deployment

In an Avaya Workspaces for Call Center Elite deployment, you need to install one to three media servers depending on your feature requirements.

The following table lists the number of media servers that you can install as a part of your deployment:

Quantity	Software Platform
1	Avaya Aura® Communication Manager
1	Avaya Breeze® platform
1	Avaya Aura® Web Gateway

For information about how to install and configure Avaya Aura® Media Server, see Deploying Avaya Breeze® platform.

Important:

To support Web Video in Avaya Workspaces for Call Center Elite, you must install Avaya Aura® Media Server Release 8.0.

Install and configure Avaya Aura® Media Server for Avaya Aura® Web Gateway

Avaya Aura® Media Server supports standard media processing features. For Avaya Aura® Media Server installation and configuration, see *Deploying Avaya Aura® Web Gateway*.

Important:

To support Web Voice in Avaya Workspaces for Call Center Elite, you must install Avaya Aura® Media Server Release 7.8 with Profile 1.

For this release, Avaya Aura® Web Gateway uses REST instead of SIP to communicate with Avaya Aura® Media Server. Therefore, Avaya Aura® Media Server requires enrollment with System Manager and configuration for REST operations. For more information, see the section about the deployment of Avaya Aura® Media Server in *Deploying Avaya Aura® Web Gateway*.

For more information about how to install, update, implement, and administer Avaya Aura® Media Server, see:

- *Deploying and Updating Avaya Aura® Media Server Appliance*
- *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS*
- *Implementing and Administrating Avaya Aura® Media Server*

Changing the default password in Avaya Aura® Media Server

About this task

After the installation of Avaya Aura® Media Server, you must change the default password.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server FQDN>:8443/emlogin`

2. On the login page, in the **User ID** field, type `admin` as the default user name.
3. In the **Password** field, type `Admin123$` as the default password.
4. Click **Sign In**.
5. Change the default password on the initial login.
6. **(Optional)** On the Avaya Aura® Media Server Element Manager interface, click **Account Management** > **Policies**, and change the required value in the fields in the Password area.
7. Click **Save**.

Installing Avaya Aura® Media Server updates

About this task

Perform the following procedure to update the system software and the Avaya Aura® Media Server software. These updates are available in the ISO format.

Before you begin

For the latest software version, install the latest patches after you install the OVA.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **Tools** > **Manage Software** > **Updates**.
4. In the Upload Updates area, click **Choose File**.
5. Browse and select the system software ISO file and click **Upload**.
6. Accept the license agreement on the completion of the upload process.
7. In the Upload Updates area, click **Choose File**.
8. Browse and select the Avaya Aura® Media Server software ISO file and click **Upload**.
9. Accept the license agreement on the completion of the upload process.
10. Click **Install Updates**.

    The upgrade process takes several minutes to complete.

Setting up the Avaya Aura® Media Server cluster

Procedure

1. On the primary Avaya Aura® Media Server, in your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **Cluster Configuration** > **Server Designation**.
4. Note the UUID.
5. Select the **Enable Replication Account** check box.
6. In the **Username** field, type `repluser`.
7. In the **Password** field, type `replpass`.

8. Click **Save**.
9. Confirm the Avaya Aura® Media Server restart.
10. On the secondary Avaya Aura® Media Server, in your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

    `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`
11. On the login page, enter the login credentials and click **Sign In**.
12. On the Avaya Aura® Media Server Element Manager interface, click **Cluster Configuration** > **Server Designation**.
13. In the **Role** field, select `Secondary`.
14. In the **Primary Server UUID** field, enter the UUID you note from the primary server.
15. In the **Primary Server Address** field, enter the IP address of the primary server.
16. Select the **Enable Replication Account** check box.
17. In the **Username** field, type `repluser`.
18. In the **Password** field, type `replpass`.
19. Click **Save**.
20. Confirm the Avaya Aura® Media Server restart.
21. On the standard Avaya Aura® Media Server, in your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

    `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`
22. On the login page, enter the login credentials and click **Sign In**.
23. On the Avaya Aura® Media Server Element Manager interface, click **Cluster Configuration** > **Server Designation**.
24. In the **Role** field, select `Standard`.
25. On the primary server, click **Cluster Configuration** > **Server Designation**.
26. In the Standard Designation area, verify that all servers are listed.
27. On the primary server, click **System Status** > **Cluster Status** to reverify all servers.

Enrolling Avaya Aura® Media Server with System Manager

About this task

Use this procedure to enroll Avaya Aura® Media Server with System Manager.

Before you begin

Add an entry to map System Manager FQDN to its IP address.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **Security** > **System Manager** > **Enrollment**.
4. On the System Manager Enrollment page, enter names and descriptions for the Avaya Aura® Media Server node and Avaya Aura® Media Server cluster.

   For clustered systems, you must enter the name and description of each node in the cluster.

5. Click **Next**.
6. Enter the FQDN of System Manager.

   Important:

   Do not enter the IP address instead of FQDN.

7. Enter the administrator user name and password for System Manager.
8. Click **Next**.
9. Select the option for creating a new System Manager signed certificates and click **Next**.
10. Enter the details of the certificate.
11. Select the **Include Subject Alternative Name with IP address** check box.
12. Include Subject Alternative Name with FQDN.
13. Enter the System Manager enrollment password.

    On the completion of the enrollment, Avaya Aura® Media Server Element Manager automatically logs you out.

    Enrollment switches the Avaya Aura® Media Server to a single sign-on mode. Therefore, you must log in to Avaya Aura® Media Server Element Manager through System Manager.

14. **(Optional)** To enable standard login to Avaya Aura® Media Server Element Manager, click **Account Management** > **Policies** and set the **Authentication and authorization source** to `Avaya Aura® Media Server`.

Configuring security certificates

About this task

Use this procedure to configure security certificates for Avaya Aura® Media Server nodes.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **Security** > **Certificate Management** > **Key Store**.
4. In the Service Profiles area, click **Assign**.
5. For each field, select the System Manager-generated certificate.

   The System Manager-generated certificate ends with `_signed`.

6. Click **Save**.
7. Click **Confirm** to restart.
8. Repeat Steps 1 through 7 for all Avaya Aura® Media Server nodes.

Configuring Avaya Aura® Media Server

About this task

You must perform the following configuration procedure on the primary Avaya Aura® Media Server node for clustered systems. After you complete these configurations on the primary node, they are automatically propagated to the other Avaya Aura® Media Server nodes in the cluster.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **Licensing** > **General Settings**.
4. In the **Server Host Name or IP Address** field, enter the IP address of System Manager.
5. Click **Save**.
6. Restart the Avaya Aura® Media Server node.
7. Log in to Avaya Aura® Media Server Element Manager.
8. On the Avaya Aura® Media Server Element Manager interface, click **Licensing** > **Monitoring**.
9. Verify that the **License Status** field is set to `License Acquired`.
10. Click **System Configuration** > **Network Settings** > **General Settings**.
11. In the SOAP area, in the **Trusted Nodes** field, enter the IP address of System Manager.

12. In the Connection Security area, in the **TLS Version** field, select `TLSv1.2`.
13. In the Connection Security area, clear the **Verify Host Name of TLS Client Connections** check box.
14. Click **Save**.
15. Click **System Configuration** > **Signaling Protocols** > **REST** > **General Settings**.
16. Clear the **Basic Authentication** check box.
17. Click **Save**.
18. Click **System Configuration** > **Server Profile** > **General Settings**.
19. Select the **Video Media Processor** check box.
20. Click **Save**.
21. Click **System Status** > **Element Status**.
22. Click **Restart**.
23. Click **Confirm** to restart.

Assigning a location to media servers

About this task

Use this procedure to assign a location to media servers in System Manager.

Procedure

1. On the System Manager web console, click **Elements** > **Media Server** > **Server Administration**.
2. Verify the entry for each installed media server.
3. Select the entry for a media server and click **Edit**.
4. In the **Location** field, assign the appropriate location to the media server.
5. Repeat Steps 3 and 4 for all media servers.

Configure Avaya Aura® Media Server for Avaya Aura® Web Gateway

The configuration of Avaya Aura® Media Server for Avaya Aura® Web Gateway includes the following:

- Configure Avaya Aura® Media Server for Web Voice.
- Create the Avaya Aura® Media Server content namespace and group if they do not already exist, and upload media prompts into the namespace.

  Without the sample media files for Web Voice, you cannot route Video contacts.

Note:

For PSTN calls, Avaya Aura® Media Server for Avaya Aura® Web Gateway is not required. Customers can have IVR on Experience Portal to play wait treatment and route the call to an agent.

Configuring audio codecs for Web Voice in Avaya Aura® Media Server

About this task

Use this procedure to configure audio codecs for Web Voice in Avaya Aura® Media Server for Avaya Breeze® platform.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **System Configuration** > **Media Processing** > **Audio Codes**.
4. Use the **Up** button to move the G.711-ULAW and G.711-ALAW codecs to the top of the **Enabled** list.
5. Click **Save**.

Configuring server profile and video codecs for Web Video

About this task

Use this procedure to configure server profile and video codecs for Web Video.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **System Configuration** > **Service Profile** > **General Settings**.
4. Select the **Firewall NAT Tunneling Media Processor** and **Video Media Processor** check boxes.
5. Click **System Configuration** > **Service Profile** > **Advanced Settings**.
6. Select the following check boxes:
   - **Firewall NAT Tunneling Media Processor**
   - **Media Server**

- **Reporting Agent**
- **SIP UserAgent**
- **Video Media Processor**
- **VoiceXML Interpreter**

7. Click **Save**.

Configuring network settings

About this task

Use this procedure to configure network settings for Avaya Aura® Media Server.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **System Configuration** > **Network Settings** > **General Settings**.
4. Select the following check boxes:
   - **Verify Host Name on HTTPS Client Connections**
   - **Verify Host Name of the Remote DB secure connection**
5. Click **Save**.

Configuring signaling protocols

About this task

Use this procedure to configure signaling protocols in Avaya Aura® Media Server.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the login page, enter the login credentials and click **Sign In**.
3. On the Avaya Aura® Media Server Element Manager interface, click **System Configuration** > **Signaling Protocols** > **SIP** > **Nodes and Routes**.
4. On the SIP Nodes and Routes page, in the Trusted Nodes area, verify the Avaya Aura® Web Gateway IP address and cluster FQDNs.
5. Click **System Configuration** > **Signaling Protocols** > **REST** > **General Settings**.

6. Select the **Enable TLS Mutual Authentication** check box.
7. Click **Save**.

Secure Real-Time Protocol configuration

Configuring SRTP in Avaya Aura® Web Gateway

About this task

Use this procedure to configure Best Effort or Enforced Secure Real-Time Protocol (SRTP) in Avaya Aura® Web Gateway.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. On the Avaya Aura® Web Gateway administration portal, click **Security Settings** > **Session Security**.
3. In the **SIP and SRTP Security Policy** field, select `Best Effort`.

   Important:

   If required, use `Enforced`.

4. Click **Save**.

Configuring SRTP in Avaya Aura® Media Server

About this task

Use this procedure to configure Best Effort or Enforced Secure Real-Time Protocol (SRTP) in Avaya Aura® Media Server.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the Avaya Aura® Media Server Element Manager interface, click **System Configuration** > **Media Processing** > **Media Security**.
3. In the **Security Policy** field, select `BEST EFFORT`.

   Important:

   If required, use `SECURITY ENFORCED`.

4. Click **Save**.

Configuring SRTP in Communication Manager

About this task

Use this procedure to configure Best Effort or Enforced Secure Real-Time Protocol (SRTP) in Communication Manager.

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Identify the Far-end Network Region assigned to the signaling group intended to process calls from Avaya Aura® Web Gateway.
3. Identify the ip-codec-set associated with the Far-end Network Region that you identify.
4. Run the **`change ip-codec-set <codec set number used by the SIP signaling group>`** command.
5. On page 1, ensure that the **Encrypted SRTCP** field is set to `Encrypted SRTCP: best-effort`.

```
Media Encryption                    Encrypted SRTCP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: 2-srtp-aescm128-hmac32
 3: none
```

Important:

If required, use **`enforce-unenc-srtcp`**.

Configuring SRTP in Avaya Aura® Session Border Controller

About this task

Use this procedure to configure Enforced Secure Real-Time Protocol (SRTP) in Avaya Aura® Session Border Controller.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. In the navigation pane, click **Domain Policies** > **Media Rules**.
4. Select the required media rule and click **Edit**.
5. On the Encryption tab, in the Audio Encryption and Video Encryption areas, ensure that the **Preferred Formats** field includes the SRTP format.
6. Click **Finish**.

Avaya Aura® Web Gateway deployment and configuration

Avaya Workspaces for Call Center Elite requires Avaya Aura® Web Gateway to provide Avaya WebRTC Connect Signaling Gateway services to Video-enabled SIP agents through a browser endpoint.

Prerequisites for Avaya Aura® Web Gateway

The following are the prerequisites for Avaya Aura® Web Gateway:

- Avaya Aura® Media Server
- LDAP/Active Directory

  You can also use a shared Active Directory.

  Ensure that you use the same groups for **User Role** and **Administrator Role** created on LDAP. See LDAP Preconfiguration on page 23 and Installing Avaya Aura Device Services on page 29.
- System Manager details
- Avaya Aura® Device Services

Important:

To support external mobile client access for Voice and Video, you must install the latest compatible patch of Avaya Aura® Web Gateway over Avaya Aura® Web Gateway 3.8.

Deploying Avaya Aura® Web Gateway

For more information about how to deploy and administer Avaya Aura® Web Gateway, see the following documents on Avaya Support website at http://support.avaya.com:

- *Deploying the Avaya Aura® Web Gateway*
- *Administering the Avaya Aura® Web Gateway*

Important:

- Use lowercase FQDNs and hostnames while deploying Avaya Aura® Web Gateway.
- To use Avaya Aura® Web Gateway, you must have a valid license installed in System Manager. If you do not have a previously installed license, generate a new license and load the license in System Manager.

Adding a device to System Manager

About this task

Use this procedure to add the Avaya Aura® Web Gateway element in System Manager.

Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, click **New**.

   The New Elements page opens.

3. In the General section, in the **Type** field, select `Avaya Aura Web Gateway`.
4. In the **Name** field, enter the name of your device.
5. In the **Node** field, enter the IP address of your device.
6. In the Access Profile section, click **New**.
7. For **Access Profile Details**, in the **Name** field, type `SSO`.
8. In the **Access Profile Type** field, select `EMURL`.
9. In the **Host** field, enter the FQDN of the server.
10. In the **Port** field, type `8445`.
11. In the **Path** field, type `/admin`.
12. Click **Save**.
13. Click **Commit**.

Configuring Avaya Aura® Web Gateway

About this task

Use this procedure to configure Avaya Aura® Web Gateway.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. Log on to Avaya Aura® Web Gateway administration portal with the credentials of the user assigned to the admin group on LDAP.

   Use the complete login name in the `user@domain` format.

3. In the navigation pane, click **General Network Settings** > **System Manager**.
4. In the **FQDN** field, enter the FQDN of System Manager.
5. In the **Protocol** field, select `https`.
6. In the **Username** field, enter the user name of the System Manager administrator account.
7. In the **Password** field, enter the password of the System Manager administrator account.
8. Click **Save**.
9. In the navigation pane, click **General Network Settings** > **Device Services**.
10. In the **FQDN** field, enter the FQDN of Avaya Aura® Device Services and click **Save**.
11. In the navigation pane, click **General Network Settings** > **LDAP Configuration**.
12. Enter the appropriate value in all fields.

    To enter the value in the fields, see the Avaya Aura® Device Services LDAP configuration.

13. Enter the appropriate value in the **Base Context DN**, **Administrator Role**, and **User Role** fields and click **Save**.
14. In the navigation pane, click **General Network Settings** > **Media Services**.
15. Verify that the page displays the details of the dedicated Avaya Aura® Media Server for Avaya Aura® Web Gateway.
16. In the navigation pane, click **Security Settings** > **HTTP Clients**.
17. In the **REST** field, change the value to `OPTIONAL` and click **Save**.
18. In the navigation pane, click **External Access** > **Guest SIP Proxy**.
19. In the Guest SIP Domain area, in the **Default Guest Sip Domain** field, enter the appropriate SIP domain and click **Save**.
20. In the Guest SIP Proxy area, click **Add**.
21. In the **SIP Address** field, enter the SIP IP Address of Session Manager.
22. In the **Weight** field, type `100`.
23. In the **SIP Port** field, type `5061`.
24. In the **SIP Protocol** field, select `TLS`.
25. In the **Location** field, select the appropriate location.
26. Click **Save**.
27. In the navigation pane, click **Security Settings** > **Trusted Hosts**.
28. In the Trusted Hosts area, add the following entries by clicking **Add**:
    - IP address of Avaya Aura® Device Services
    - FQDN of Avaya Aura® Device Services
    - IP address of Session Manager
    - Self FQDN of Avaya Aura® Web Gateway
    - FQDN of System Manager
    - FQDNs of Avaya Breeze® platform nodes
29. Click **Save**.
30. In the navigation pane, click **Security Settings** > **Session Security**.
31. In the Cipher Support area, select all ciphers for media encryption and click **Save**.
32. In the navigation pane, click **Advanced** > **CORS Configuration**.
33. Select the **Enable Cross-Origin Resource Sharing** and **Allow access from any origin** check boxes and click **Save**.
34. In the navigation pane, click **General Network Settings** > **Location**.
35. In the Web Gateway Locations area, select a location for the Web Gateway and click **Save**.

The location might take some time to appear because it must be synchronized from System Manager.

36. In the navigation pane, click **Advanced** > **Media Settings** > **Audio**.
37. In the WebRTC Audio Codecs area, verify that G711A and G711MU are prioritized and placed on the top.
38. In the navigation pane, click **Advanced** > **Media Settings** > **Video**.
39. In the **Call Maximum Video Bandwidth (kbps)** field, change the value to `768`.

Verifying the components connected to Avaya Aura® Web Gateway

About this task

Use this procedure to verify that all configured components are successfully connected to Avaya Aura® Web Gateway.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. Log on to Avaya Aura® Web Gateway administration portal with the credentials of the user assigned to the admin group on LDAP.

   Use the complete login name in the `user@domain` format.

3. In the content pane, in the Solution Servers area, verify that the status of the following components is `Connected`:

   - **LDAP Configuration**
   - **Device Services**
   - **System Manager**
   - **Media Services**

   Note:

   Proceed to the next step only after you verify that the four components are displayed as connected and green.

Configuring Avaya Aura® for Avaya Aura® Web Gateway

About this task

Use this procedure to configure Avaya Aura® components for Avaya Aura® Web Gateway through System Manager.

Procedure

1. On the System Manager web console, click **Elements** > **Media Server** > **Application Assignment**.
2. On the Application Assignment page, select **Avaya Aura Web Gateway** and click **Edit**.
3. Select an available Avaya Aura® Media Server cluster that does not have an asterisk (*) mark.
4. Click **Commit**.
5. On the System Manager web console, click **Elements** > **Media Server** > **Server Administration**.
6. On the Server Administration page, ensure that the location of each media server in the new Avaya Aura® Web Gateway media server cluster is set.
7. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`
8. Log on to Avaya Aura® Web Gateway administration portal with the credentials of the user assigned to the admin group on LDAP.

   Use the complete login name in the `user@domain` format.
9. In the navigation pane, click **Security Settings** > **Trusted Hosts**.
10. In the Trusted Hosts area, add the following entries by clicking **Add**:
    - FQDN of Avaya Aura® Web Gateway
    - FQDN of Avaya Aura® Device Services
    - FQDN of System Manager
    - FQDNs of the media servers in the cluster assigned to Avaya Aura® Web Gateway
11. On the System Manager web console, click **Elements** > **Routing** > **SIP Entities**.
12. On the SIP Entities page, click **New**.
13. In the **Name** field, enter a name for the Avaya Aura® Web Gateway entity.
14. In the **IP address** field, enter the IP address of Avaya Aura® Web Gateway.
15. In the **Type** field, select `SIP Trunk`.
16. In the **Location** field, select the appropriate location.
17. In the **Time Zone** field, select the appropriate time zone.
18. In the **SIP Link Monitoring** field, select `Link Monitoring Disabled`.
19. In the **CRLF Keep Alive Monitoring** field, select `CRLF Monitoring Disabled`.
20. In the Entity Links area, click **Add**.
21. In the **SIP Entity 1** field, select the Session Manager SIP entity.

22. In the **SIP Entity 2** field, select the Avaya Aura® Web Gateway SIP entity.
23. Click **Commit**.

Enabling Token Service and TestApp

About this task

Use this procedure to enable Token Service and TestApp in Avaya Aura® Web Gateway.

Procedure

1. Using an SSH client, log on to Avaya Aura® Web Gateway.
2. Run the following commands:

   ```
   cdto active
   cd mss/*/telportal/webapps
   sudo mv devclient.undeploy devclient.war; sudo mv token-generation-service.undeploy token-generation-service.war
   ```

3. Run the following command to restart Avaya Aura® Web Gateway services:

   ```
   svc CSA restart
   ```

   The restart process might take several minutes to complete.

Testing the installation of Avaya Aura® Web Gateway

About this task

Use this procedure to test the installation of Avaya Aura® Web Gateway through TestApp.

Before you begin

Enable Avaya Aura® Web Gateway Token Service and TestApp.

Procedure

1. In your web browser, enter the following URL to start Avaya Aura® Web Gateway TestApp:

   `https://<Avaya Aura Web Gateway_FQDN>/devclient/testapp/index.html`

   Where *<Avaya Aura Web Gateway_FQDN>* is the FQDN of the Avaya Aura® Web Gateway server.

2. When prompted, enter the login credentials of a valid agent as defined in LDAP.

   The browser displays the Avaya Aura® Web Gateway TestApp console with some text in green.

3. Type **ac<return>**.

   The browser displays several lines of text in green.

   For example, `<= serviceStatusChanged: calls service activated`.

The lines indicate that Avaya Aura® Web Gateway is installed correctly.

4. For audio calls, run the following command:

   call <destination number> audio

5. For video calls, run the following command:

   call <destination number> video

Enabling port for remote access on Avaya Aura® Web Gateway HTTP Reverse Proxy

About this task

This procedure is required only for remote worker agent configuration.

Procedure

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

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. On the Avaya Aura® Web Gateway administration portal, click **External Access** > **HTTP Reverse Proxy**.
3. Select the **Use Front-end Host from a client request** check box.
4. Select the **Enable port for remote access** check box.
5. In the **Front-end port for remote access** field, enter a port number.

   For example, enter a port number similar to 8444.

   Avaya Aura® Web Gateway uses this port number to distinguish between clients on the internal network and external clients on the internet. Internal clients use the standard 443 port whereas external clients such as Browsers, Android, and iOS use the port specified in this field to access Avaya Aura® Web Gateway. Based on the port number, Avaya Aura® Web Gateway sets the media paths.

6. Click **Save**.

Avaya Aura® Web Gateway authorization

When a request is made between a client and the Avaya Aura® Web Gateway server, an authorization token is passed with the request. This authorization token is the same token that Avaya Workspaces passes with the requests to Unified Agent Controller (UAC). The authorization is handled through AuthorizationService.

Avaya Aura® Web Gateway is a third-party server. Therefore, you must configure the Avaya Breeze® platform Authorization Certificate on Avaya Aura® Web Gateway. However, it creates a conflict because each Avaya Breeze® platform node in the cluster has a different Authorization Certificate.

When load balancing is enabled between the nodes, some requests are rejected because they cannot be authorized. Therefore, you must create a single, shared certificate that you can use for authorization on all nodes in the cluster.

Enabling authorization on Avaya Aura® Web Gateway

Before you begin

Obtain the Avaya Breeze® platform authorization certificate file in the `.PEM` format.

For information about how to create the common certificate, import it in Avaya Breeze® platform nodes, and export the Avaya Breeze® platform authorization Identity Certificate see:

- Creating the common certificate on page 26
- Importing the authorization certificate on page 27
- Exporting the Avaya Breeze platform Authorization Identity Certificate on page 28

Procedure

1. On the Avaya Aura® Web Gateway 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**.

Configure the voice media path

Configuring codecs in Avaya Aura® Web Gateway

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. On the Avaya Aura® Web Gateway administration portal, click **Advanced** > **Media Settings** > **Audio**.
3. In the **SIP Audio Coded Preference** drop-down list, select Custom.
4. From the **SIP Audio Codecs** list, remove all codecs except your preferred, such as, G711 codec (G711A or G711MU), OPUS codec (OPUS Wideband or OPUS Narrowband).
5. From the **WebRTC Audio Codecs** list, remove all codecs except your preferred, such as, G711 codec (G711A or G711MU), OPUS codec (OPUS Wideband or OPUS Narrowband).
6. Click **Save**.

7. On the Avaya Aura® Web Gateway administration portal, click **Advanced** > **Media Settings** > **Video**.
8. From the **SIP Video Codecs** list, remove all codecs except the H264 codec.
9. From the **WebRTC Video Codecs** list, remove all codecs except the H264 codec.
10. Set the **Call Maximum Video Bandwidth** field to `768` kbps.
11. Click **Save**.

Prioritizing codecs in Avaya Aura® Media Server

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the Avaya Aura® Media Server Element Manager interface, click **System Configuration** > **Media Processing** > **Audio Codecs**.
3. Use the **Up** button to move your preferred G711 codec or OPUS codec to the top of the **Enabled** list.
4. Click **Save**.

Prioritizing codecs in Communication Manager

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Identify the Far-end Network Region assigned to the signaling group intended to process calls from Avaya Aura® Web Gateway.
3. Identify the ip-codec-set associated with the Far-end Network Region that you identify.
4. Run the **`change ip-codec-set <codec set number used by the SIP signaling group>`** command.
5. On page 1, in the **Audio Codec** area, verify that your preferred codec, such as G711 codec (G.711A or G.711MU), OPUS codec (OPUS Wideband or OPUS Narrowband) is at number on the list.
6. **(Optional)** If the signaling group intended to process calls from or to Avaya Breeze® platform is different, repeat Step 1 to Step 5 for that signaling group.

Creating Avaya WebRTC Connect agents for Avaya Workspaces for Call Center Elite Solution

Creating a user in Active Directory

About this task

Use this procedure to create a user in Active Directory who can act as a general user for Avaya Aura® Device Services, and can also administer Avaya Aura® Device Services and Avaya Aura® Web Gateway.

Procedure

1. Log in to the server containing the Active Directory.
2. Click **Start** > **Administrative Tools** > **Active Directory Users and Computers**.
3. In the navigation pane, expand the domain that you created for the users.
4. Right-click the Active Directory organizational unit (OU) and click **New** > **User**.
5. In the **New Object - User** dialog box, in the **First name** field, enter the first name of the user.
6. In the **Last name** field, enter the surname of the user.
7. In the **User logon name** field, enter the user name.
8. Click **Next**.
9. In the **Password** field, enter a password for the user.
10. In the **Confirm Password** field, re-enter the password.
11. Clear the **User must change password at next logon** check box.
12. Select the **Password never expires** check box.
13. Click **Next**.
14. Click **Finish**.

    The server displays the new user in the list in the content pane.
15. In the content pane, right-click the new user and click **Add to a group**.
16. In the Select Groups dialog box, add the user to the standard users group and the appropriate administrator group, and click **OK**.

    For more information, see LDAP Preconfiguration on page 23.

Create a user in System Manager and Communication Manager

The following are the two methods that you can use to create users:

- Create users manually through System Manager.

- Create an XML file containing users and import them into System Manager through the bulk import utility.

Creating a user through System Manager

About this task

Use this procedure to manually create a user through System Manager.

Procedure

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

   System Manager displays the User Profile | Add page.
3. In the **Last Name** field, enter the surname of the user.
4. In the **First Name** field, enter the first name of the user.
5. In the **Login Name** field, enter the login name of the user, including the domain name.
6. In the **Password** and **Confirm Password** fields, enter the password.
7. Click **Commit and Continue**.
8. In the **Communication Profile Password** field, click **Edit** and enter the password.
9. In the Communication Address area, click **New**.
10. Leave the **Type** field as `Avaya SIP`.
11. In the **Fully Qualified Address** field, enter the SIP address of the user station.
12. In the **Domain** field, choose the appropriate domain.
13. Click **Add**.
14. Select the **Session Manager Profile** check box.
15. In the Primary Session Manager field, select the primary Session Manager.
16. In the **Originating Sequence** and **Terminating Sequence** fields, select the option which was added in **Elements** > **Session Manager** > **Application Configuration** > **Application Sequences**.
17. In the **Home Location** field, select the appropriate value.
18. Select the **CM Endpoint Profile** check box.
19. In the **System** field, select `CM system`.
20. Leave the **Profile Type** field as `Endpoint`.
21. In the **Extension** field, enter the SIP address of the user station.
22. In the **Template** field, select the appropriate template based on the version of Communication Manager.
23. **(Optional)** In the **Preferred Handle** field, select the communication address of the user.

24. Click **Endpoint editor** in the **Extension** field.
25. On the General Options tab, ensure that the **Type of 3PCC Enabled** field is set to `Avaya`.
26. On the Feature Options tab, select the **IP Softphone** check box.
27. Select the **IP Video Softphone** check box.
28. Clear the **H.320 Conversion** check box.
29. Select the **Direct IP-IP Audio Connections** check box.
30. On the Button Assignment tab, set the button features in the following way:

Button Feature	Argument-1	Argument-2
manual-in		
call-appr		
call-appr		
call-appr		
aux-work		
auto-in		
agnt-login		

31. Click **Done**.
32. Click **Commit**.

Creating System Manager users through bulk import utility

About this task

Use this procedure to create System Manager users through bulk import utility.

Procedure

1. Create a user bulk import XML file using the template.
2. Save the XML file on your local machine.
3. On the System Manager web console, click **Users** > **User Management** > **Manage Users**.
4. On the Manage Users page, click **More Actions** > **Import Users**.
5. Click **Browse** and select the XML file.
6. Click **Import**.

Synchronizing users with Avaya Control Manager

About this task

The synchronization process synchronizes the user information from Communication Manager in to the Avaya Control Manager database.

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\Services\ACCCM Synchronizer` folder.
3. Right-click the `NAV360_Synchronizer` file and click **Run as administrator**.
4. In the **Type Sync** field, select `CM`.
5. In the **Objects to Synchronize**, select `Extension`.
6. In the **Locations to Synchronize**, select `appropriate location`.
7. Click **Start** to start the synchronization process.
8. Click **Yes** on the confirmation screen.

Configuring VDNs and vectors for Avaya Workspaces for Call Center Elite

About this task

Use this procedure to configure basic VDNs and vectors which you can use to route calls to Avaya Workspaces for Call Center Elite agents.

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. On page 1 of the VECTOR DIRECTORY NUMBER screen, in the **Name** field, enter the name of the VDN.
3. In the **Destination** field, set the destination to a vector number which is not in use.

   This example uses 5.
4. In the **Allow VDN Override** field, type `y`.

   This allows this VDN to be overridden and routed to another VDN.

```
display vdn 3011                                          Page   1 of   3
                          VECTOR DIRECTORY NUMBER

                            Extension: 3011
                                Name*: Helpdesk
                          Destination: Vector Number        5
                  Attendant Vectoring? n
                 Meet-me Conferencing? n
                   Allow VDN Override? y
                                  COR: 1
                                   TN*: 1
                             Measured: none


        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:



* Follows VDN Override Rules
```

5. Save the settings.
6. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
7. 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.
8. On page 1 of the CALL VECTOR screen, in the **Name** field, enter the name of the vector.
9. 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
```

10. Save the settings.
11. Run **`add vdn next or add vdn n`**.

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

    This example uses 2.
14. In the **Allow VDN Override** field, type `n`.

```
display vdn 3007                                          Page   1 of   3
                          VECTOR DIRECTORY NUMBER

                            Extension: 3007
                                Name*: Sales Support
                          Destination: Vector Number        2
                 Attendant Vectoring? n
               Meet-me Conferencing? n
                 Allow VDN Override? n
                                COR: 1
                                TN*: 1
                           Measured: external


        VDN of Origin Annc. Extension*:
                            1st Skill*:
                            2nd Skill*:
                            3rd Skill*:



* Follows VDN Override Rules
```

15. Save the settings.
16. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
17. 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.
18. On page 1 of the CALL VECTOR screen, in the **Name** field, enter the name of the vector.
19. 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 Avaya Workspaces for Call Center 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
```

20. Save the settings.

Creating a user in Avaya Control Manager

Before you begin

- Ensure that Avaya Workspaces for Call Center Elite Cluster 1 is in running and accepting state.
- For each Avaya WebRTC Connect agent, ensure the following on Communication Manager:
  - On page 2 of the STATION screen, the **Auto Answer** field is set to `none`.
  - On page 1 of the AGENT LOGINID screen, the **Auto Answer** field is set to `none`.

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.
3. Click **Add**.
4. In the Available applications section, select the **Workspaces for Elite** check box .
5. In the **Team** field, select the available option.
6. In the **First Name (English)** field, enter the first name of the user in English.
7. In the **Surname (English)** field, enter the surname of the user in English.
8. In the **LDAP Username** field, enter the LDAP user name of the user.

   The LDAP user name must be in the username@domain.com format. This user name is used for logging on to Avaya Workspaces.

9. In the **Username** field, enter a user name.

   In this release, the user name is the internal handle.

10. In the **Password** field, enter a password.

    This password is used for logging on to Avaya Control Manager.

11. In the **Confirm Password** field, re-enter the password.
12. In the **AVAYA Login** field, enter the AgentID of the agent.

    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. In the **Extension** field, enter the SIP station associated with this agent that was created in Creating a user through System Manager on page 56 Synchronizing users with Avaya Control Manager on page 57.

    Note:

    This station should exist on System Manager: Communication Manager and Avaya Control Manager.

    This is used when logging on to Avaya Workspaces.

    Note:

    You must enter a value in this field only if the agent has to handle Voice contacts.

14. Click **Save**.
15. Scroll to the right and select the **Avaya Oceana** tab.
16. Select the **Allow browser only login** check box.
17. Click **Skills** tab.
18. Select the skill number associated with the VDN created.

    See Configuring VDNs and vectors for Avaya Workspaces for Call Center Elite on page 58.

19. Click **Save**.

Logging in to Avaya Workspaces

About this task

Use this procedure to log in to Avaya Workspaces.

Before you begin

Get the Avaya Workspaces URL from your supervisor.

Procedure

1. Access Avaya Workspaces by using the URL that you received from your supervisor.

The URL is in the format: `https://CLUSTER-FQDN/services/UnifiedAgentController/workspaces/#/login`.

2. In the **Username** field, type your user name.

   Important:

   Avaya Workspaces supports the use of apostrophe (') in the username.

3. In the **Password** field, type your password.
4. Click **Sign in**.

   Avaya Workspaces displays the Activate Agent screen.

5. In the **Profile** field, select the profile.
6. In the **Extension** field, type the extension.
7. Click **Activate**.

   Avaya Workspaces displays a blank interaction area with the option to Start Work, and the Team and Welcome widgets.

8. Click **Start Work**.

   Note:

   If enabled by your administrator, on the interaction area you can click **Go Ready** to start work in the Ready state, or click **Go Not Ready** to start work in the Not Ready state.

   This places you in the Ready or Not Ready state for customer interactions. Avaya Workspaces queues interactions in the **Interaction** area.

Chapter 6: Configure Avaya Workspaces for Call Center Elite Solution with web and mobile voice calls

Overview

Customers can make web and mobile voice calls to agents having Avaya Agent for Desktop or Avaya one-X® Agent softphones running on their computers. This chapter provides information on configuring Avaya Workspaces for Call Center Elite with web and mobile voice calls.

Configuration checklist

Use the following checklist to configure Avaya Workspaces for Call Center Elite with web and mobile voice calls so that phone-enabled agents can answer web and mobile voice calls:

No.	Task	Description	✔
1	Install and configure Avaya Aura® Web Gateway and Avaya Aura® Media Server.	See the following: • Avaya Aura Web Gateway deployment and configuration on page 46. • Avaya Aura Media Server deployment on page 35.	
2	Install and configure web and mobile applications to make anonymous calls to Avaya Aura® Web Gateway.	See Install and configure web and mobile applications on page 66.	
3	Install and configure Avaya Aura® Session Border Controller to enable calls from the public internet.	See Install and configure Avaya Aura® Session Border Controller on page 72.	

Table continues…

No.	Task	Description	✔
4	Configure Avaya Breeze® platform so that voice calls can be anchored on Avaya Breeze® platform with wait treatment.	See Install and configure Avaya Aura Media Server for Avaya Aura Web Gateway on page 36.	
5	Configure the voice media path.	See the following:. • Configuring codecs in Avaya Aura Web Gateway on page 53. • Prioritizing codecs in Avaya Aura Media Server on page 54. • Prioritizing codecs in Communication Manager on page 54.	

Install and configure web and mobile applications

Avaya supplies the following web and mobile applications or reference clients for making anonymous calls to Avaya Aura® Web Gateway:

- Javascript reference client for web browsers.

  Web browsers are supported on the Windows desktop platform only.
- iOS reference client for iOS devices.
- Android reference client for Android devices.

To make anonymous calls to Avaya Aura® Web Gateway, you must install and configure these applications on the relevant platform.

Installing the Javascript reference client

Before you begin

Ensure that you have the free base-level registered membership of Avaya DevConnect Program. For information about Avaya DevConnect, see *Avaya DevConnect Program Guide* available on https://support.avaya.com.

Procedure

1. Download the JavaScript reference client from the Avaya DevConnect portal at http://www.avaya.com/devconnect.
2. To use the JavaScript reference client, extract the relevant archive retrieved in the previous step and copy the folder to the customer-provided web server.

   The JavaScript reference client is now reachable on the customer web server.

Configuring the Javascript reference client and making a call

Before you begin

Ensure that the following certificates are installed on the client computer:

- A root certificate from Certificate Authority (CA), for example System Manager CA certificate.
- A common identity certificate for Avaya Breeze® nodes. For example, certificate created in common certificate section.
- A trust certificate for Avaya Aura® Device Services using the link: `https://<Avaya Aura Device Services_FQDN>/acs/resources`.
- A trust certificate for Avaya Aura® Web Gateway using the link: `https://<Avaya Aura Web Gateway_FQDN/csa/resources/tenants/default`.

Procedure

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

   `https://<IP Address>/ReferenceClient/index.html`

   `<IP Address>` is the IP address of the server hosting the Reference Client web application.
2. Click the Hamburger menu on the right-top corner.
3. Click **Settings**.
4. Select **Elite**.
5. On the CLIENT CONFIG tab, in the **Display Name** field, enter the customer display name.
6. In the **From Address** field, enter the customer address.

   The from address must be a numeric value. If you do not specify a from address, it is randomly assigned for each call.
7. In the **Destination Address** field, enter the VDN number to make a VDN call or add Station ID to Agent ID to make a direct call to the agent. See Configuring VDNs and vectors for Avaya Workspaces for Call Center Elite on page 58.
8. In the **Context (Optional)** field, enter the customer specific information.
9. In the **Topic (Optional)** field, enter the customer specific information.
10. Click the SERVICE tab and enter appropriate values in the **Priority**, **Locale**, and **Strategy** fields.
11. Click the RESOURCE tab.
12. In the **Source Name** field, enter the name of the Voice provider to which the agent is associated.
13. In the **Resource Id** field, enter the Native Resource ID of the agent.

    To get the Voice provider name, you must log on to Avaya Control Manager and access the Providers tab on the Workspaces for Elite Server Edit page. Perform this step only if you use the Specified (Required or Preferred) Resource or Coverage feature for Web Voice.

14. Click the AAWG CONFIG tab.
15. In the **AAWG Server Address** field, enter the FQDN of the Avaya Aura® Web Gateway server.
16. In the **AAWG Server Port** field, type one of the following values:
    - Type `80` for HTTP.
    - Type `443` for HTTPS.
17. Configure the **Use HTTPS** field to enable security.
18. Click the TOKEN CONFIG tab.
19. In the **Token Service Address** field, enter the FQDN of the webserver that is hosting the token service.
20. In the **Token Service Port** field, enter the port number of the webserver that is hosting the token service.
21. In the **Use HTTPs** field, select the checkbox for HTTPS.

    Important:

    This is based on the protocol that the reference client uses when connecting to the webserver that is hosting the token service.
22. In the **Token Server Url Path** field, enter the URL path to connect to the token service hosted on a webserver
23. Click **Save**.
24. Click the Hamburger menu and then select **Home**.
25. Click **(+)** icon.
26. Click **Start Audio** or **Start Video** to initiate a Avaya WebRTC Connect Voice/Video call .

    For a Voice call, ensure that you have a microphone connected and the browser has access to the microphone. For a Video call, ensure that you have a webcam and a microphone connected and the browser has access to the webcam and the microphone.

Installing the iOS reference client

Before you begin

- Ensure that you have the free base-level registered membership of Avaya DevConnect Program. For information about Avaya DevConnect, see *Avaya DevConnect Program Guide* available on https://support.avaya.com.
- Ensure that the following certificates are installed and trusted on the iOS device:
  - A root certificate from Certificate Authority (CA), for example System Manager CA certificate.
  - A common identity certificate for Avaya Breeze® nodes. For example, certificate created in common certificate section.

- A trust certificate for Avaya Aura® Device Services using the link: `https://<Avaya Aura Device Services_FQDN>/acs/resources`.
- A trust certificate for Avaya Aura® Web Gateway using the link: `https://<Avaya Aura Web Gateway_FQDN/csa/resources/tenants/default`.

Procedure

1. Download the iOS reference client from the Avaya DevConnect portal at http://www.avaya.com/devconnect.
2. To use the iOS reference client, extract the relevant archive retrieved in the previous step on an Apple Mac and double-click on the `.xcodeproj` file.

   This opens the XCode project. The reference client can now be built from XCode and can be run on an iOS device.

Configuring the iOS reference client and making a call

Procedure

1. Open the iOS reference client for Avaya Workspaces for Call Center Elite.
2. Click the Hamburger menu on the right-top corner.
3. Click **Settings**.
4. Select **Elite**.
5. On the CLIENT CONFIG tab, in the **Display Name** field, enter the customer display name.
6. In the **From Address** field, enter the customer address.

   The from address must be a numeric value. If you do not specify a from address, it is randomly assigned for each call.
7. In the **Destination Address** field, enter the VDN number to make a VDN call or add Station ID to Agent ID to make a direct call to the agent. See Configuring VDNs and vectors for Avaya Workspaces for Call Center Elite on page 58.
8. In the **Context (Optional)** field, enter the customer specific information.
9. In the **Topic (Optional)** field, enter the customer specific information.
10. Click the SERVICE tab and enter appropriate values in the **Priority**, **Locale**, and **Strategy** fields.
11. Click the RESOURCE tab.
12. In the **Source Name** field, enter the name of the Voice provider to which the agent is associated.
13. In the **Resource Id** field, enter the Native Resource ID of the agent.

    To get the Voice provider name, you must log on to Avaya Control Manager and access the Providers tab on the Workspaces for Elite Server Edit page. Perform this step only if you use the Specified (Required or Preferred) Resource or Coverage feature for Web Voice.

14. Click the AAWG CONFIG tab.
15. In the **AAWG Server Address** field, enter the FQDN of the Avaya Aura® Web Gateway server.
16. In the **AAWG Server Port** field, type one of the following values:
    - Type `80` for HTTP.
    - Type `443` for HTTPS.
17. Configure the **Use HTTPS** field to enable security.
18. Click the TOKEN CONFIG tab.
19. In the **Token Service Address** field, enter the FQDN of the webserver that is hosting the token service.
20. In the **Token Service Port** field, enter the port number of the webserver that is hosting the token service.
21. In the **Use HTTPs** field, select the checkbox for HTTP.

    Important:

    This is based on the protocol that the reference client uses when connecting to the webserver that is hosting the token service.
22. In the **Token Server Url Path** field, enter the URL path to connect to the token service hosted on a webserver.
23. Click **Save**.
24. Click the Hamburger menu and then select **Home**.
25. Click **(+)** icon.
26. Click **Start Audio** or **Start Video** to initiate a Avaya WebRTC Connect Voice/Video call .

    For a Voice call, ensure that you have a microphone connected and the browser has access to the microphone. For a Video call, ensure that you have a webcam and a microphone connected and the browser has access to the webcam and the microphone.

Installing the Android reference client

Before you begin

- Ensure that you have the free base-level registered membership of Avaya DevConnect Program. For information about Avaya DevConnect, see *Avaya DevConnect Program Guide* available on https://support.avaya.com.
- Ensure that the following certificates are installed and trusted on the Android device:
  - A root certificate from Certificate Authority (CA), for example System Manager CA certificate. .
  - A trust certificate for Avaya Aura® Device Services using the link: `https://<Avaya Aura Device Services_FQDN>/acs/resources`.

- A trust certificate for Avaya Aura® Web Gateway using the link: `https://<Avaya Aura Web Gateway_FQDN/csa/resources/tenants/default`.

Procedure

1. Download the Android reference client from the Avaya Devconnect portal at http://www.avaya.com/devconnect.
2. To use the Android reference client, extract the relevant archive retrieved in the previous step.
3. Using Android Studio, import the project.

   The reference client can now be built from Android Studio and can be run on an Android device.

Configuring the Android reference client and making a call

Procedure

1. Open the Avaya Workspaces for Call Center Elite Android Reference Client.
2. Click the Hamburger menu on the right-top corner.
3. Click **Settings**.
4. Select **Elite**.
5. On the CLIENT CONFIG section, in the **Display Name** field, enter the customer display name.
6. In the **From Address** field, enter the customer address.

   The from address must be a numeric value. If you do not specify a from address, it is randomly assigned for each call.
7. In the **Destination Address** field, enter the VDN number to make a VDN call or add Station ID to Agent ID to make a direct call to the agent. See Configuring VDNs and vectors for Avaya Workspaces for Call Center Elite on page 58.
8. In the **Context (Optional)** field, enter the customer specific information.
9. In the **Topic (Optional)** field, enter the customer specific information.
10. Click the SERVICE tab and enter appropriate values in the **Priority**, **Locale**, and **Strategy** fields.
11. Click the RESOURCE tab.
12. In the **Source Name** field, enter the name of the Voice provider to which the agent is associated.
13. In the **Resource Id** field, enter the Native Resource ID of the agent.

    To get the Voice provider name, you must log on to Avaya Control Manager and access the Providers tab on the Workspaces for Elite Server Edit page. Perform this step only if you use the Specified (Required or Preferred) Resource or Coverage feature for Web Voice.

14. Click the AAWG CONFIG tab.
15. In the **AAWG Server Address** field, enter the FQDN of the Avaya Aura® Web Gateway server.
16. In the **AAWG Server Port** field, type one of the following values:
    - Type `80` for HTTP.
    - Type `443` for HTTPS.
17. Configure the **Use HTTPS** field to enable security.
18. Click the TOKEN CONFIG tab.
19. In the **Token Service Address** field, enter the FQDN of the webserver that is hosting the token service.
20. In the **Token Service Port** field, enter the port number of the webserver that is hosting the token service.
21. In the **Use HTTPs** field, select the checkbox for HTTP.

    Important:

    This is based on the protocol that the reference client uses when connecting to the webserver that is hosting the token service.
22. In the **Token Server Url Path** field, enter the URL path to connect to the token service hosted on a webserver.
23. Click **Save**.
24. Click the Hamburger menu and then select **Home**.
25. Click **(+)** icon.
26. Click **Start Audio** or **Start Video** to initiate a Avaya WebRTC Connect Voice/Video call .

    For a Voice call, ensure that you have a microphone connected and the browser has access to the microphone. For a Video call, ensure that you have a webcam and a microphone connected and the browser has access to the webcam and the microphone.

Install and configure Avaya Aura® Session Border Controller

Note:

This section is applicable only for remote worker agent configuration.

Avaya Workspaces for Call Center Elite requires Avaya Aura® Session Border Controller to enable calls from the public internet. Therefore, you must install Avaya Aura® Session Border Controller as part of your solution. For information about how to install Avaya Aura® Session Border Controller, see *Deploying Avaya Session Border Controller on a Hardware Platform*.

For information about how to configure Avaya Aura® Session Border Controller to enable calls from the public internet, complete the tasks described in this section.

Configuring Avaya Aura® Session Border Controller networks

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **Network Management** > **Interfaces**.
3. On the Interfaces page, enable the following interfaces:
   - A1 internal interface
   - B1 external interface
4. On the Networks tab, configure the following networks:
   - A1 internal network
   - B1 external network
5. For external web and mobile access, assign IP addresses to each network as follows:

   External IP addresses:
   - One IP address for the Avaya Aura® Web Gateway reverse proxy
   - One IP address for the TURN relay service

   Internal IP addresses:
   - One IP address for the Avaya Aura® Web Gateway reverse proxy
   - One IP address for the TURN relay service

Creating a reverse proxy policy

Procedure

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

Creating a reverse proxy service for Avaya Aura® Web Gateway

Before you begin

Create a reverse proxy policy through the EMS web interface, ensuring that the **Allow Web Socket** field for the reverse proxy policy is set to `Y`.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.
3. On the Reverse Proxy tab, click **Add**.

   Add Reverse Proxy Profile page opens.
4. In the **Service Name** field, type the reverse proxy profile name.
5. Select the **Enabled** check box.
6. In the **Listen IP** field, click the external IP address of Avaya SBC.
7. In the **Listen Port** field, type the port number as 443.
8. In the **Listen Protocol** field, click `HTTP/HTTPS`.
9. In the **Listen TLS Profile** field, click the relevant TLS Profile.
10. In the **Server Protocol** field, click `HTTP/HTTPS`.
11. In the **Connect IP** field, click the internal IP address of Avaya SBC.
12. In the **Reverse Proxy Policy Profile** field, click the reverse proxy policy that you created.
13. In the **Server Addresses** field, type *<Avaya Aura Web Gateway IP/FQDN>*:*<port number>*.

    The value of *<Avaya Aura Web Gateway IP/FQDN>* must be based on the value that you used in the SAN name while creating the TLS certificate.

    The value of *<port number>* must be same as the port number configured in the **Front-end port for remote access** field on the HTTP Reverse Proxy page in Avaya Aura® Web Gateway. Avaya Aura® Web Gateway uses this port to identify requests from an external or remote user.

    To go to the HTTP Reverse Proxy page, you must log on to the Avaya Aura® Web Gateway administration portal and click **External Access** > **HTTP Reverse Proxy**.
14. Click **Finish**.

Deploying Identity Certificate

Perform the following procedures to deploy Identity Certificate on Avaya Aura® Session Border Controller.

Creating the common client certificate

About this task

Use this procedure to create the common client certificate that you require while creating a client profile for Avaya Aura® Session Border Controller.

Procedure

1. Log on to Avaya Aura® System Manager.
2. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
3. In the navigation pane, in the RA Functions section, click **Add End Entity**.
4. In the **End Entity Profile** field, select `INBOUND_OUTBOUND_TLS`.
5. In the **Username** field, enter a user name.

   For example, SBCINT.
6. 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.
7. In the **Confirm Password** field, re-enter the password.
8. In the **CN, Common name** field, enter the FQDN of Session Border Controller.

   For example, Subject: CN=SBCFQDN.apac.avaya.com, CN=SBCFQDN.apac.avaya.com, OU=SDP, O=AVAYA, C=US
9. In the first **DNS Name** field, enter the domain name of the first node of the cluster.

   For example, DNS1: apac.avaya.com.
10. In the second **DNS Name** field, enter the domain name of the second node of the cluster.

    For example, DNS2: apac.avaya.com
11. In the **IP Address** field, enter the IP address of the internal interface.
12. In the **Token** field, select `P12 file`.
13. Click **Add**.
14. **Create a keystore**: On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
15. In the navigation pane, click **Public Web**.
16. On the EJBCA welcome page, in the navigation pane, click **Create Keystore**.
17. On the Keystore Enrollment page, enter the user name and password that you specified while creating the end entity.
18. Click **OK**.
19. Select the **Key Length** as 2048 bits.

20. Click **Enroll**.
21. Save the certificate file.

Creating the common server certificate

About this task

Use this procedure to create the common server certificate that you require while creating a server profile for Avaya Aura® Session Border Controller.

Procedure

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

   For example, SBCEXT.
5. 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.
6. In the **Confirm Password** field, re-enter the password.
7. In the **CN, Common name** field, enter the FQDN of Session Border Controller.

   For example, Subject: CN=SBCFQDN.apac.avaya.com, CN=SBCFQDN.apac.avaya.com, OU=SDP, O=AVAYA, C=US
8. In the first **DNS Name** field, enter the enter the FQDN for Avaya Aura® Web Gateway of the cluster.

   For example, DNS1: AAWG.apac.avaya.com.
9. In the second **DNS Name** field, enter the domain name of the second node of the cluster.

   For example, DNS2: apac.avaya.com
10. In the **IP Address** field, enter the IP address of the external interface.
11. In the **Token** field, select `P12 file`.
12. Click **Add**.
13. **Create a keystore**: On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
14. In the navigation pane, click **Public Web**.
15. On the EJBCA welcome page, in the navigation pane, click **Create Keystore**.
16. On the Keystore Enrollment page, enter the user name and password that you specified while creating the end entity.

17. Click **OK**.
18. Select the **Key Length** as 2048 bits.
19. Click **Enroll**.
20. Save the certificate file.

Creating a client profile for the Avaya Aura® Web Gateway reverse proxy

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management** > **Client Profiles**.
3. On the Client Profiles page, click **Add**.
4. In the **Profile Name** field, type the name of the profile.
5. In the **Certificate** field, select a certificate.

   The certificate must include the internal interface IP that you need to specify in the **Connect IP** field while creating a reverse proxy service for Avaya Aura® Web Gateway.
6. In the **Peer Verification** field, click **Required**.
7. In the **Peer Certificate Authority** field, use the CA that is used to sign your certificates.
8. In the **Verification Depth** field, type `1`.
9. Keep the default values in the other fields.
10. Click **Finish**.

Creating a server profile for the Avaya Aura® Web Gateway reverse proxy

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management** > **Server Profiles**.
3. On the Server Profiles page, click **Add**.
4. In the **Profile Name** field, type the name of the profile.
5. In the **Certificate** field, select a certificate.

   The certificate must include:

   - The external interface IP that you need to specify in the **Listen IP** field while creating a reverse proxy service for Avaya Aura® Web Gateway
   - Avaya Aura® Web Gateway FQDN because external clients use this FQDN to access Avaya Aura® Web Gateway
6. In the **Peer Verification** field, click **None**.
7. Keep the default values in the other fields.
8. Click **Finish**.

Generating Identity Certificate from the System Manager Certificate Authority

About this task

Use this procedure generate Identity Certificate from the System Manager Certificate Authority (CA) in the P12 format.

Procedure

1. **Create an end entity**: Log on to Avaya Aura® System Manager.
2. On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
3. In the navigation pane, in the RA Functions section, click **Add End Entity**.
4. In the **End Entity Profile** field, select `INBOUND_OUTBOUND_TLS`.
5. In the **Username** field, enter a user name.
6. 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 generating the certificate.
7. In the **Confirm Password** field, re-enter the password.
8. Complete any other fields that you want in your certificate.
9. In the **CN, Common name** field, enter the FQDN of Session Border Controller.
10. In the **IP Address** field, enter the IP address of Session Border Controller.
11. In the **Certificate Profile** field, select `ID_CLIENT_SERVER`.
12. In the **CA** field, select `tmdefaultca`.
13. In the **Token** field, select `P12 file`.
14. Click **Add**.
15. **Create a keystore**: On the System Manager web console, click **Services** > **Security** > **Certificates** > **Authority**.
16. In the navigation pane, click **Public Web**.
17. On the EJBCA welcome page, in the navigation pane, click **Create Keystore**.
18. On the Keystore Enrollment page, enter the user name and password that you specified while creating the end entity.
19. Click **OK**.
20. Select the **Key Length** as 2048 bits.
21. Click **Enroll**.
22. Save the certificate file in the P12 format.

Extracting the certificate and private key in Session Border Controller

About this task

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

Procedure

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

   `openssl pkcs12 –in <filename>.p12 -out <filename>.pem -nokeys –clcerts`

3. Run the following command to extract the private key from the P12 file:

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

Installing the client and server certificates on Session Border Controller

About this task

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

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management** > **Certificates**.
3. On the Certificates page, click **Install**.
4. In the **Type** field, select `Certificate`.
5. In the **Name** field, type the name of the profile.

   For example, sbc_cert.

6. In the **Certificate File** field, select the certificate that you extracted in Session Border Controller.

   For example, cert.pem.

7. In the **Key** field, select **Upload Key File**.
8. Select the private key that you extracted in Session Border Controller.
9. In the **Key Passphrase** field, enter the password that you provided during private key generation.
10. Click **Upload File**.
11. Check the certificate to verify all details that you provided when creating the p12 file.
12. Click **Install**.

Configure TURN for Avaya WebRTC Connect

Avaya Workspaces for Call Center Elite supports both Client side TURN and server side TURN for WebRTC Connect calls from the public internet. Avaya recommends the use of Client side TURN unless there is a specific reason where Server side TURN is required. Follow one of the procedures below to configure either WebRTC Connect Client side TURN OR WebRTC Connect Server side TURN.

Configure Avaya WebRTC Connect Client Side TURN

Creating a server profile for the TLS TURN relay

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management** > **Server Profiles**.
3. Click **Add** to add a new TLS server profile.
4. In the **Profile Name** field, enter a name for the profile.
5. In the **Certificate** field, select appropriate certificate.

   Important:

   Ensure that the certificate associated with the profile includes the external (B1) Interface IP. This B1 IP acts as an listen IP for the TLS client TURN requests. Hence, port 443 must not be in use on this B1 IP for any other SBC function such as reverse proxy.
6. In the **Peer Verification** field, select **None**.
7. Leave all others fields to default values.
8. Click **Next**.
9. Click **Finish**.

Adding a TURN/STUN service for Avaya WebRTC Connect clients

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **DMZ Services** > **TURN/STUN Service** > **TURN/STUN Profiles**.
3. On the TURN/STUN Profiles tab, click **Add**.
4. In the **Profile Name** field, type an appropriate profile name.
5. In the **UDP Listen Port** field, type `3478`.
6. In the **TCP/TLS Listen Port** field, type `443`.
7. In the **TLS Server Profile** field, select the profile created in Creating a server profile for the TLS TURN relay on page 80.

8. In the **Media Relay Port Range** field, type a value between 50000 to 55000.
9. In the **Authentication** field, enable the authentication.
10. In the **Client Authentication** field, enable the authentication.
11. In the **Realm** field, specify the SIP domain.
12. In the **UDP Relay** field, enable the UDP relay.
13. Click **Finish**.
14. On the TURN Relay tab, click **Add**.
15. In the **Listen IP** field, enter the external interface IP configured on Avaya Aura® Session Border Controller that external clients use.
16. In the **Media Relay IP** field, enter the internal IP configured on Avaya Aura® Session Border Controller that Avaya Aura® Web Gateway and Avaya Aura® Media Server use for media.
17. Keep the **Service FQDN** field blank.
18. In the **TURN/STUN Profile** field, select the TURN/STUN profile that you created.
19. Click **Finish**.

Enabling Avaya WebRTC Connect Client Side TURN on Web Gateway

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. Log on to Avaya Aura® Web Gateway administration portal with your administrator credentials.
3. On the Avaya Aura® Web Gateway administration portal, click **External Access** > **Session Border Controller** .
4. Select the **Enable TURN in WebRTC Client** check box.
5. Click **Save**.

Creating a server profile for the Avaya Aura® Session Border Controller signaling interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management** > **Server Profiles**.
3. On the Server Profiles page, click **Add**.
4. In the **Profile Name** field, type the name of the profile.
5. In the **Certificate** field, select a certificate.

The certificate must include the internal interface IP that is to be used to communicate with Session Manager.

6. In the **Peer Verification** field, click **None**.
7. Keep the default values in the other fields.
8. Click **Finish**.

Creating the Avaya Aura® Session Border Controller signaling interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select your ASBCE.
3. In the navigation pane, click **Network & Flows** > **Signaling Interface**.
4. Click **Add**.
5. In the **Name** field, enter an appropriate name for the signaling interface.
6. In the **IP Address** field, enter the internal IP address that is allocated for communication with Session Manager.
7. In the **TCP Port** field, type `5060`.
8. Keep the **UDP Port** field blank.
9. In the **TLS Port** field, type `5061`.
10. In the **TLS Profile** field, select the server profile that you created for the Avaya Aura® Session Border Controller signaling interface.
11. Keep the default values in the other fields.
12. Click **Finish**.

Configuring the Avaya Aura® Session Border Controller external media interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select your ASBCE.
3. In the navigation pane, click **Network & Flows** > **Media Interface**.
4. Click **Add**.
5. In the **Name** field, enter an appropriate name for the media interface.
6. In the **IP Address** field, enter the external IP address that is allocated for external media.
7. Leave the **TLS Profile** field as None.

8. In the **Port Range** field, enter any value between 35000 to 40000.
9. Keep the default values in the other fields.
10. Click **Finish**.

Configuring the Avaya Aura® Session Border Controller internal media interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select your ASBCE.
3. In the navigation pane, click **Network & Flows** > **Media Interface**.
4. Click **Add**.
5. In the **Name** field, enter an appropriate name for the media interface.
6. In the **IP Address** field, enter the internal IP address that is allocated for internal media.
7. In the **Port** field, enter any value between 35000 to 40000.
8. Leave the **TLS Profile** field as None.
9. Keep the default values in the other fields.
10. Click **Finish**.

Creating an application rule

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select your ASBCE.
3. In the navigation pane, click **Domain Policies** > **Application Rules**.
4. In the Application Rules pane, click **Add**.
5. On the Application Rule page, enter a name for the new application rule and click **Next**.
6. Select the following check boxes:
   - **In**
   - **Out**
   - **Audio**
   - **Video**
7. In the **Maximum Concurrent Sessions** field, enter the appropriate value.
8. In the **Maximum Sessions Per Endpoint** field, enter the appropriate value.
9. Keep the default values in the other fields.

10. Click **Finish**.

Creating an endpoint policy group

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select your ASBCE.
3. In the navigation pane, click **Domain Policies** > **End Point Policy Group**.
4. In the Application pane, click **Add**.
5. In the **Group Name** field, type a name for the new policy group, and click **Next**.
6. Assign the newly created video-enabled application rule to the policy group.
7. Click **Finish**.

Creating a client profile for the Avaya Aura® Session Border Controller signaling interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select your ASBCE.
3. In the navigation pane, click **TLS Management** > **Client Profiles**.
4. On the Client Profiles page, click **Add**.
5. In the **Profile Name** field, type the name of the profile.
6. In the **Certificate** field, select a certificate.

   The certificate must include the internal interface IP that is to be used to communicate with Session Manager.
7. In the **Peer Verification** field, click **Required**.
8. In the **Peer Certificate Authority** field, use the CA that is used to sign your certificates.
9. In the **Verification Depth** field, type `1`.
10. Keep the default values in the other fields.
11. Click **Finish**.

Creating an interworking profile without remote Avaya Aura® Session Border Controller

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select your ASBCE.

3. In the navigation pane, click **Configuration Profiles** > **Server Interworking**.
4. In the Interworking Profiles area, select **avaya-ru** and click **Clone**.

   The EMS web interface displays the Clone Profile dialog box.
5. In the **Clone Name** field, enter a name for the new profile.

   For example, avaya-no-sbc.
6. Click **Finish**.
7. In the Interworking Profiles area, select the new profile.
8. Click the **Advanced** tab and click **Edit**.

   The EMS web interface displays the Editing Profile dialog box.
9. Ensure that the **Has Remote SBC** check box is cleared.
10. Click **Finish**.

Adding a server configuration for Avaya Aura® Web Gateway

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select your ASBCE.
3. In the navigation pane, click **Services** > **SIP Servers**.
4. Click **Add**.
5. In the **Profile Name** field, type a name for the new server profile and click **Next**.
6. In the **Server Type** field, select `Trunk Server`.
7. Leave the **SIP Domain** field blank.
8. In the **DNS Query Type** field, select `NONE/A`.
9. In the **TLS Client Profile** field, enter the client profile that you created for the Avaya Aura® Session Border Controller signaling interface.
10. In the **IP Addresses/FQDNs** field, enter the IP address of the Avaya Aura® Web Gateway server node.
11. In the **Port** field, type `5061`.
12. In the **Transport** field, select `TLS`.
13. Keep the default values in the other fields and click **Next**.
14. On the Add Server Configuration Profile - Advanced page, select the **Enable Grooming** check box.
15. In the **Interworking Profile** field, select the newly created interworking profile with remote SBC disabled.
16. Keep the default values in the other fields.

17. Click **Finish**.
18. If the Avaya Aura® Web Gateway server is part of a cluster, repeat this procedure to add a server configuration for each server node in the cluster.

    Do not add Server Configuration for the shared virtual IP.

Adding a server configuration for Session Manager

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select your ASBCE.
3. In the navigation pane, click **Services** > **SIP Servers**.
4. Click **Add**.
5. In the **Profile Name** field, type a name for the new server profile and click **Next**.
6. In the **Server Type** field, select `Trunk server`.
7. Leave the **SIP Domain** field blank.
8. In the **DNS Query Type** field, select `NONE/A`.
9. In the **TLS Client Profile** field, enter the client profile that you created for the Avaya Aura® Session Border Controller signaling interface.
10. In the **IP Addresses/FQDNs** field, enter the IP address of the Session Manager server.
11. In the **Port** field, type `5061`.
12. In the **Transport** field, select `TLS`.
13. Keep the default values in the other fields and click **Next**.
14. On the Add Server Configuration Profile - Advanced page, select the **Enable Grooming** check box.
15. In the **Interworking Profile** field, select the newly created interworking profile with remote SBC disabled.
16. Keep the default values in the other fields.
17. Click **Finish**.

Adding a server flow for Avaya Aura® Web Gateway

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select your ASBCE.
3. In the navigation pane, click **Network & Flows** > **End Point Flows** > **Server Flows**.
4. Click **Add**.

5. In the **Flow Name** field, type an appropriate name for the flow.
6. In the **Server Configuration** field, select the configuration for the Avaya Aura® Web Gateway server node.
7. Keep the default values for the **URI Group**, **Transport**, and **Remote Subnet** fields.
8. In the **Received Interface** field, specify the internal SIG interface.
9. In the **Signaling Interface** field, specify the internal SIG interface.
10. In the **Media Interface** field, specify the external media interface.
11. In the **End Point Policy Group** field, select the video-enabled endpoint policy group.
12. Keep the default values in the other fields.
13. Click **Finish**.
14. If the Avaya Aura® Web Gateway server is part of a cluster, repeat this procedure to add a server flow for each server node in the cluster.

Adding a server flow for Session Manager

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select your ASBCE.
3. In the navigation pane, click **Network & Flows** > **End Point Flows** > **Server Flows**.
4. Click **Add**.
5. In the **Flow Name** field, type an appropriate name for the flow.
6. In the **SIP Server Profile** field, select the configuration for the Session Manager server.
7. Keep the default values for the **URI Group**, **Transport**, and **Remote Subnet** fields.
8. In the **Received Interface** field, specify the internal SIG interface.
9. In the **Signaling Interface** field, specify the internal SIG interface.
10. In the **Media Interface** field, specify the internal media interface.
11. In the **End Point Policy Group** field, select the video-enabled endpoint policy group.
12. Keep the default values in the other fields.
13. Click **Finish**.

Configuring Avaya Aura® Session Border Controller for load monitoring

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select your ASBCE.

3. In the navigation pane, click **Network & Flows** > **Advanced Options** > **Load Monitoring**.
4. Click **Add**.
5. In the **Load Balance Type** field, select `INTERNAL`.
6. In the **Transport** field, select `TCP`.
7. In the **Listen IP** field, select an internal SIG IP that can be used.
8. Click **Finish**.

Adding Avaya Aura® Session Border Controller as a SIP entity in System Manager

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **SIP Entities**.
2. On the SIP Entities page, click **New**.
3. In the **Name** field, enter a name for the SIP entity.
4. In the **FQDN or IP Address** field, enter the IP address of the Avaya Aura® Session Border Controller internal interface that you specified while creating the Avaya Aura® Session Border Controller signaling interface. For more information see, Creating the Avaya Aura Session Border Controller signaling interface on page 82.
5. In the Type field, enter **SIP Trunk**.
6. Configure the appropriate **Location** and **Time Zone**.
7. Leave all other fields with default values.
8. In **Entity Links** click **Add**.
9. Modify the Entity Link name if required.
10. In the **SIP Entity 1** field, select the Session Manager entity.
11. In the **Protocol** field, select `TLS`.
12. In the **Port** field, enter `5061`.
13. In the **SIP Entity 2** field, select the Session Border Controller entity.
14. In the **Port** field, enter `5061`.
15. In the **Connection Policy** field, select `trusted`.
16. Click **Commit**.

Adding the Avaya Aura® Session Border Controller configuration to Avaya Aura® Web Gateway

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. On the Avaya Aura® Web Gateway administration portal, click **External Access** > **Session Border Controller**.
3. Click **Add**.
4. In the **SIP Address** field, type the address of the Avaya Aura® Session Border Controller internal interface that you specified while creating the Avaya Aura® Session Border Controller signaling interface.
5. In the **SIP Port** field, type `5061`.
6. In the **SIP Protocol** field, select `TLS`.
7. In the **HTTP Address** field, type the address of the Avaya Aura® Session Border Controller internal interface that you specified while configuring Avaya Aura® Session Border Controller for load monitoring.
8. In the **HTTP Port** field, type `80` if you are using HTTP protocol or 443 if you are using HTTPS protocol.
9. In the **HTTP Protocol** field, select `http` or `https`.
10. In the **Location** field, specify the location of the Avaya Aura® Session Border Controller server.
11. Click **Save**

Chapter 7: Configure Avaya Workspaces for Call Center Elite Solution with web and mobile video calls and Avaya WebRTC Connect agents

Overview

Avaya WebRTC Connect agents can answer web and mobile video calls. This chapter provides information on configuring Avaya Workspaces for Call Center Elite with web and mobile video calls and WebRTC Connect agents.

Configuration checklist

Use the following checklist to configure Avaya Workspaces for Call Center Elite with web and mobile video calls and WebRTC Connect agents so that WebRTC Connect agents can answer web and mobile video calls:

No.	Task	Description	✔
1	Install and configure Avaya Aura® Web Gateway, Avaya Aura® Media Server, and Avaya Aura® Device Services.	See the following: • Avaya Aura Web Gateway deployment and configuration on page 46. • Avaya Aura Media Server deployment on page 35. • Avaya Aura Device Services deployment on page 29.	

Table continues…

No.	Task	Description	✔
2	Install and configure Avaya Aura® Media Server.	See Install and configure Avaya Aura Media Server for Avaya Aura Web Gateway on page 36.	
3	Configure authorization on Avaya Aura® Web Gateway.	See Avaya Aura Web Gateway authorization on page 52.	
4	Create WebRTC Connect agents that can use media in browsers.	See Creating a user in Avaya Control Manager on page 62.	
5	Configure the voice media path.	See the following:. • Configuring codecs in Avaya Aura Web Gateway on page 53. • Prioritizing codecs in Avaya Aura Media Server on page 54. • Prioritizing codecs in Communication Manager on page 54.	
6	Install and configure web and mobile applications to make anonymous calls to Avaya Aura® Web Gateway.	See Install and configure web and mobile applications on page 66.	
7	Install and configure Avaya Aura® Session Border Controller to enable calls from the public internet.	See Install and configure Avaya Aura® Session Border Controller on page 72.	
8	Create WebRTC Connect video agents.	See Create Avaya WebRTC Connect video agents on page 91.	
9	Configure the video media path.	See Configure the video media path on page 94.	

Create Avaya WebRTC Connect video agents

Important:

For Web Video, you must install Avaya Aura® Communication Manager 7.1.2 or later version.

Configuring customer options

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run the **`change system-parameters customer-options`** command.

3. On page 5, verify that the **Multimedia IP SIP Trunking** field is set to `y`.
4. Save the settings.

Configuring the signaling group for Web Video

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change signaling-group n`**.

   n is the number of the signaling group that you need to configure.
3. On the SIGNALING GROUP screen, in the **IP Video** field, type `yes`.
4. In the **Priority Video** field, type `yes`.
5. In the **Initial IP-IP Direct Media** field, type `yes`.
6. Save the settings.

Enabling Video on a Communication Manager SIP station

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change station n`**.

   n is the number of the SIP for which you want to enable Video.
3. **Page 1**: In the **IP Softphone** and **IP Video Softphone** fields, type `Y`.
4. **Page 2**: In the **H.320 Conversion** field, type `N`.
5. In the **Direct IP-IP Audio Connections** field, type `Y`.
6. Save the settings.

Enable Video for Avaya Workspaces for Call Center Elite SIP agents

In Avaya Workspaces for Call Center Elite, agents handle Video contacts using a Video enabled SIP station. Therefore, you must first configure SIP agents for Avaya Workspaces for Call Center Elite and then enable Video for those SIP agents.

Configuring a provider to support Video

Before you begin

Ensure that Avaya Workspaces for Call Center Elite Cluster 1 is in running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Custom Engagement** > **Workspace for Elite**.
2. On the Avaya Workspaces for Call Center Elite Server List page, double-click the UCAServer server.
3. Select the **Communication Manager** tab.
4. Select the check box for the Voice provider and click **Edit**.
5. Select the **Video Enabled** check box.
6. Click **Save**.

Enabling Video for an Avaya Workspaces for Call Center Elite agent

About this task

Use this procedure to upgrade an existing agent so that the agent can receive video calls.

Procedure

1. Log on to the Avaya Aura® System Manager webpage.
2. Click **Users** > **User Management** > **Manage Users**.
3. Select a user and click **Edit**.
4. Click **Session Manager Profile** and enter the required details.
5. Click **CM Endpoint Profile** and enter the required details.
6. In the **Extension field**, click the pencil icon.
7. In the **General Options** tab, in the **Type of 3PCC Enabled** field, select `Avaya`.
8. Click **Done**.

Configuring an IP network region

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change ip-network-region`**
3. **Page 1**: In the **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** fields, type `yes`.
4. Save the settings.

Configure the video media path

Configuring media servers for Web Video

About this task

Perform this procedure for all Avaya Breeze® platform and Avaya Aura® Web Gateway media servers.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager.

   `https://<AMS_EM_FQDN>:8443/emlogin/`

2. Click **System Configuration** > **Server Profile** > **General Settings**.
3. Select the **Video Media Processor** check box and click **Save**.

Configuring an IP codec set for Video

Procedure

1. Using SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Run **`change ip-codec-set`**.
3. **Page 2**: In the **Allow Direct-IP Multimedia** field, type `yes`.
4. In the **Maximum Call Rate for Direct-IP Multimedia** field, type `768 kbps`.
5. In the **Maximum Call Rate for Priority Direct-IP Multimedia** field, type `768 kbps`.
6. Save the settings.

Configuring codecs in Avaya Aura® Web Gateway

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. On the Avaya Aura® Web Gateway administration portal, click **Advanced** > **Media Settings** > **Audio**.
3. Select **Custom** in **SIP Audio Codec Preference** list.
4. From the **SIP Audio Codecs** list, remove all codecs except your preferred, such as, G711 codec (G711A or G711MU), OPUS codec (OPUS Wideband or OPUS Narrowband).
5. From the **WebRTC Audio Codecs** list, remove all codecs except your preferred, such as, G711 codec (G711A or G711MU), OPUS codec (OPUS Wideband or OPUS Narrowband).

6. Click **Save**.
7. On the Avaya Aura® Web Gateway administration portal, click **Advanced** > **Media Settings** > **Video**.
8. From the **SIP Video Codecs** list, remove all codecs except the H264 codec.
9. From the **WebRTC Audio Codecs** list, remove all codecs except the H264 codec.
10. Set the **Call Maximum Video Bandwidth** field to `768` kbps.
11. Click **Save**.

Adding the OPUS codec to the SIP Audio Codecs list

About this task

Use this procedure to add the OPUS Wideband or Narrowband codec to the SIP Audio Codecs list. You can use the similar procedure to add any of your preferred codecs.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. On the Avaya Aura® Web Gateway administration portal, click **Advanced** > **Media Settings** > **Audio**.
3. In the **SIP Audio Coded Preference** field, select `Custom`.
4. In the **SIP Audio Codec** field, based on your requirement, select `Opus Wideband` or `Opus Narrowband` and click **Add**.
5. In the **SIP Audio Codecs** list, verify the OPUS codec.
6. Click **Save**.

Adding the OPUS codec to the WebRTC Audio Codecs list

About this task

Use this procedure to add the OPUS Wideband or Narrowband codec to the WebRTC Audio Codecs list. You can use the similar procedure to add any of your preferred codecs.

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. On the Avaya Aura® Web Gateway administration portal, click **Advanced** > **Media Settings** > **Audio**.
3. In the **WebRTC Audio Codec** field, select `Opus` and click **Add**.

4. In the **OPUS Profile** field, based on your requirement, select `Wide Band` or `Narrow Band` and click **Add**.
5. In the **WebRTC Audio Codecs** list, verify the OPUS codec.
6. Click **Save**.

Configuring the OPUS codec in Avaya Aura® Media Server

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`

2. On the Avaya Aura® Media Server Element Manager interface, click **System Configuration** > **Media Processing** > **Audio Codecs**.
3. In the **Available** list, based on your requirement, select the OPUS Wideband or Narrowband codec and click **Add** to move the codec to the **Enabled** list.
4. Use the **Up** button to move the codec to the top of the **Enabled** list.
5. Click **Save**.

Configuring the OPUS codec in Communication Manager

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Identify the Far-end Network Region assigned to the signaling group intended to process calls from Avaya Aura® Web Gateway.
3. Identify the ip-codec-set associated with the Far-end Network Region that you identify.
4. Run the **`change ip-codec-set <codec set number used by the SIP signaling group>`** command.
5. On page 1, in the **Audio Codec** area, based on your requirement, verify that the OPUS Wideband or Narrowband codec is present the list.
6. To prioritize, ensure that your codec is at the top of the list.
7. **(Optional)** If the signaling group intended to process calls from or to Avaya Breeze® platform is different, repeat Step 1 to Step 5 for that signaling group.

Configuring the OPUS codec in Avaya Aura® Session Border Controller

About this task

Use this procedure to configure the OPUS Wideband or Narrowband codec in Avaya Aura® Session Border Controller. You can use the similar procedure to configure any of your preferred codecs.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. In the navigation pane, click **Domain Policies** > **Media Rules**.
4. Select the required media rule and click **Edit**.
5. Click **Codec Prioritization** > **Audio Codec** > **Edit**.
6. Select the **Codec Prioritization** check box.
7. In the **Available** list, based on your requirement, select the OPUS Wideband or Narrowband codec and click the > arrow to move the codec to the **Selected** list.
8. Select the **Allow Preferred Codecs Only** check box to allow only preferred codecs.
9. Select **Codec Prioritization** check box if you have multiple codecs and want to set the priority.

   The topmost codec gets the highest priority.
10. Click **Finish**.

Prioritizing codecs in Avaya Aura® Media Server

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<Avaya Aura Media Server_FQDN>:8443/emlogin`
2. On the Avaya Aura® Media Server Element Manager interface, click **System Configuration** > **Media Processing** > **Audio Codecs**.
3. Use the **Up** button to move your preferred G711 or OPUS codec to the top of the **Enabled** list.
4. Click **Save**.

Prioritizing codecs in Communication Manager

Procedure

1. Using an SSH client, connect to the Communication Manager System Access Terminal (SAT) interface.
2. Identify the Far-end Network Region assigned to the signaling group intended to process calls from Avaya Aura® Web Gateway.
3. Identify the ip-codec-set associated with the Far-end Network Region that you identify.
4. Run the **`change ip-codec-set <codec set number used by the SIP signaling group>`** command.
5. On page 1, in the **Audio Codec** area, verify that your preferred G711 codec (G.711A or G.711MU) or OPUS codec (OPUS Wideband or OPUS Narrowband) is at number on the list.
6. **(Optional)** If the signaling group intended to process calls from or to Avaya Breeze® platform is different, repeat Step 1 to Step 5 for that signaling group.

Chapter 8: Remote Worker Solution

Overview

Avaya Workspaces for Call Center Elite supports the remote worker functionality for Web Voice and Web Video. With this functionality, remote agents and supervisors who are located outside the contact center infrastructure can access Avaya Workspaces for Call Center Elite applications and perform their tasks.

A remote worker can be an agent or a supervisor with reporting and agent capabilities.

You must deploy Avaya Workspaces for Call Center Elite applications with the standard Avaya Aura® applications for Web Voice and Web Video with Avaya Aura® Session Border Controller. With this type of deployment, remote workers with Internet can access full remote worker capabilities from any location outside the contact center infrastructure.

To use the remote worker functionality, you must:

- Deploy Avaya Workspaces for Call Center Elite 3.8.x.
- Deploy and enable Web Voice and Web Video capabilities for all on-premise and remote workers.
- Deploy the following applications for Web Voice and Web Video:
  - Avaya Aura® Web Gateway
  - Avaya Aura® Media Server
  - Avaya Aura® Device Services
  - Avaya Aura® Session Border Controller
- Deploy a combination of on-premise workers in the firewall of Avaya Aura® Session Border Controller and remote workers outside the firewall of Avaya Aura® Session Border Controller.

Remote workers capabilities

The capabilities of remote workers are similar to standard on-premise workers.

Avaya Workspaces for Call Center Elite remote workers can perform the following operations:

- Remote Web Voice workers can receive incoming PSTN Voice calls using media in their Avaya Workspaces for Call Center Elite-supported browsers and process them through Avaya Workspaces.

  It implies that the remote workers can initiate outgoing voice contacts to reachable destinations through Avaya Workspaces.

- Remote Web Video workers can receive incoming Web Video calls using media in their Avaya Workspaces for Call Center Elite-supported browsers and process them through Avaya Workspaces.

  It implies that the remote workers can initiate outgoing video contacts to reachable destinations through Avaya Workspaces.

Avaya Workspaces for Call Center Elite remote workers can have the following roles:

Role	Description
Supervisor Agent	Can access all supported supervisor functions of Avaya Workspaces for Call Center Elite.
Agent	Can access all supported agent functions of Avaya Workspaces for Call Center Elite.
Remote Worker Agent	Can log in from outer network and support all functions of Avaya Workspaces for Call Center Elite for web voice and web video.
Administrator	Can access all access to all Avaya Workspaces administration functions, such as adding or changing the widget layouts.

Remote workers limitations

Regardless of the type and roles, remote workers:

- Cannot use Avaya telephony devices at their remote location to handle voice contacts from PSTN customers.

  Remote workers only use their browsers to handle all voice contacts.

- Cannot use the following capabilities for Web Voice:
  - DTMF

    DTMF is supported on the customer side. Customers can send DTMF with limitations.
  - Auto Answer

Remote worker solution architecture

The following diagram depicts the high-level architecture of the remote worker solution:

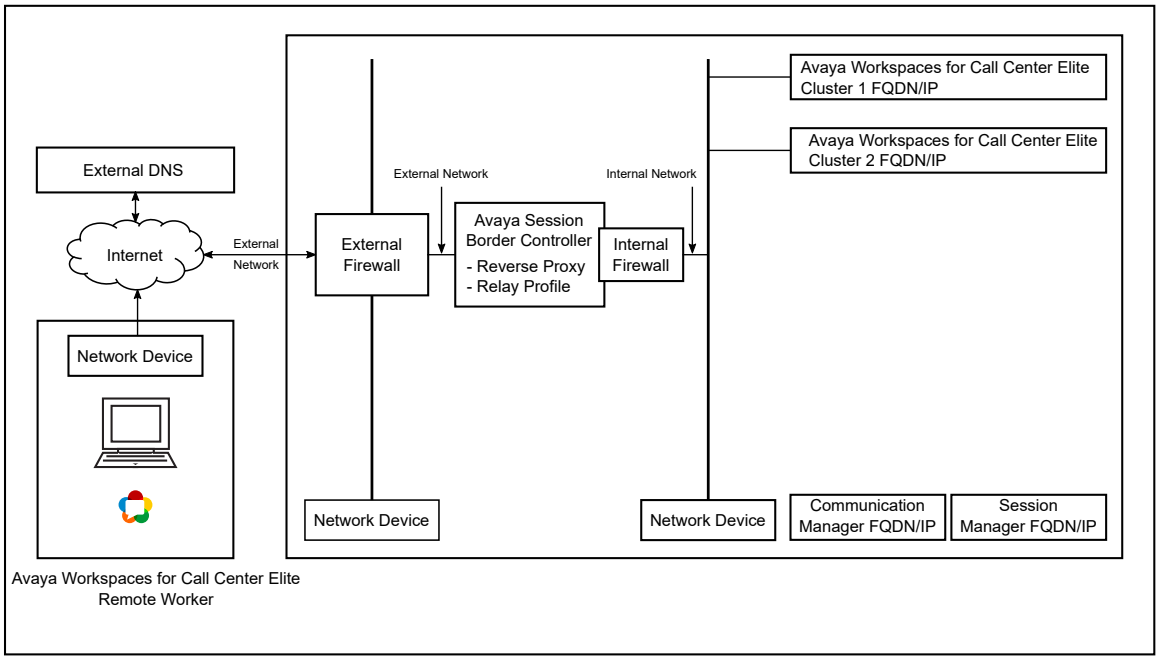


Figure 1: Remote Worker Solution

All workers in the bigger box use Avaya Workspaces for Call Center Elite FQDNs to directly access solution functionality on the internal LAN. All workers outside the bigger box are considered as external workers. The external workers must transit through firewall layers and network elements by using interfaces on the external firewall to connect to the Avaya Workspaces for Call Center Elite applications. Customers must deploy this level of infrastructure so that remote workers can get secure access to enterprise applications.

For the remote worker capability, you must deploy and provision the following:

- Avaya Aura® Session Border Controller

  You must configure and enable the following on Session Border Controller:

  - One externally facing IP address on its external (B1) side.
  - One internally facing IP address on its internal (A1) side.
  - A certificate for the B1 external interface. You use this certificate for the reverse proxy.
  - A certificate for the A1 internal interface. You use this certificate for the reverse proxy.
- External DNS capability to resolve the Avaya Workspaces for Call Center Elite FQDNs to an IP address that is accessible from the Internet.
- External firewall to provide a double layer of security (DMZ) between the Internet and the backend Avaya Workspaces for Call Center Elite servers.

  You must have an external firewall with the following configured items:

  - One external IP address on the WAN side.
  - One internal IP address on the LAN side.

You must enable the following ports on the external firewall:

- Port 443 for general signaling of the remote worker devices/clients to Avaya Workspaces for Call Center Elite AuthorizationService.
- Port 9443 for authorization of the remote worker devices/clients to contact center applications.

- Internal firewall

  You must have an internal firewall with the following configured items:

  - Up to six externally facing IP addresses on the external (WAN) side.
  - One internally facing IP address on the internal (LAN) side.

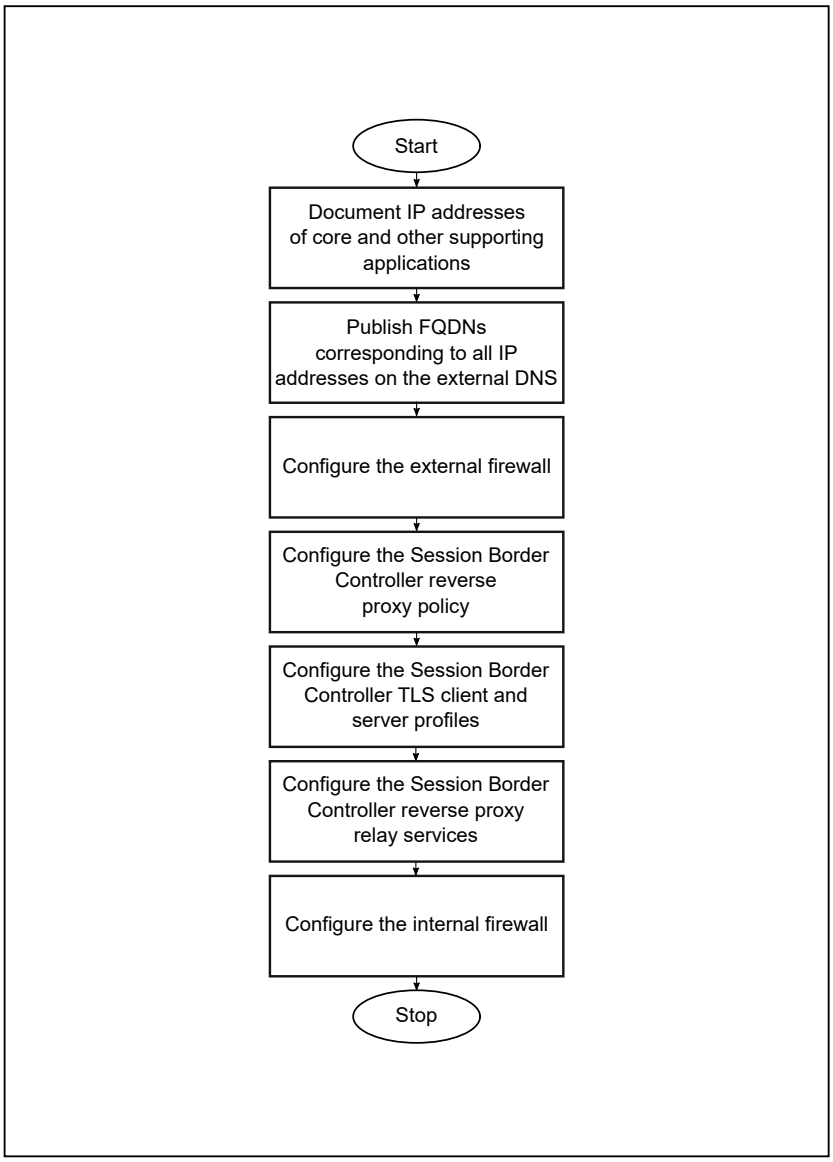
The following are the additional considerations for the remote worker solution:

- You must use the split-horizon DNS so that on-premise and remote workers can use the same FQDNs to use Avaya Workspaces for Call Center Elite. However, the FQDNs resolve to different IP addresses depending on whether the agent is remote or on-premise.
- All Avaya Workspaces for Call Center Elite FQDNs resolve to a single IP address on the external firewall and proxies are used internally to the correct Avaya Workspaces for Call Center Elite server or cluster based on the request URL from the client.
- Minimum network characteristics must be achieved with the internet connection from the remote workers to the on-premise infrastructure containing the contact center.

  Remote workers utilize Avaya Workspaces, and its performance degrades, or it becomes unresponsive on network connections with a latency greater than 300 ms Round Trip Time (RTT). Remote workers must have a reliable internet connection that can deliver an RTT less than 300 ms.
- Avaya Workspaces for Call Center Elite is deployed and operational for all required channels.
- On-premise agents can log in to Avaya Workspaces and process contacts.
- Avaya Workspaces for Call Center Elite must completely use secure connections:
  - The **Only allow secure web communication** check box must be selected in the cluster attributes of all Avaya Workspaces for Call Center Elite clusters.
  - The **Secure Communications** attribute must be enabled in the EliteLargeConfiguration service.
- Any screen-pops required for agents must be externalized so that they are accessible to the remote agents.

Remote worker solution process flow

The following workflow shows the sequence of tasks that you must perform to deploy the remote worker solution:



Configuration and deployment details for the remote worker solution

For successful deployment of the remote worker solution, you must gather all configuration and deployment details.

Documentation of FQDNs and IP addresses of solution interfaces

To deploy the remote worker solution, you must document FQDNs and IP addresses of Avaya Workspaces for Call Center Elite interfaces that remote workers access during normal operations.

Publishing of FQDNs external to the enterprise for remote workers

Avaya Workspaces for Call Center Elite users use FQDNs to access the functionality in the solution. In the enterprise, FQDNs are resolved to the IP addresses through the internal Domain Name Server (DNS). For example, Avaya Workspaces users access Avaya Workspaces for Call Center Elite Cluster 1 or Avaya Workspaces for Call Center Elite Cluster 2 FQDNs to login and receive basic user functionality depending on the agent footprint size.

Similar to on-premise workers, remote workers must also be able to utilize the same URLs and client requests, even though they are outside of the enterprise. Therefore, customers must publish a DNS entry for each required Avaya Workspaces for Call Center Elite FQDN that remote workers use. The number of FQDNs for publishing depends on customer configuration.

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

Function and role of the external firewall for remote workers

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

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

Function and role the reverse proxy for remote workers

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

The reverse proxy is configured with a set of rules that analyze the request URLs and allow the requests to go to the backend Avaya Workspaces for Call Center Elite servers.

.

Reverse proxy policies, TLS profiles, and relay services

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

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

For example, you must configure a relay service for Avaya Workspaces for Call Center Elite clusters containing the Authorization service.

Function and role of the internal firewall for remote workers

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

Connectivity details of remote workers

Remote workers connect to the Avaya Workspaces for Call Center Elite contact center similar to how they connect within the enterprise. They access Avaya Workspaces for Call Center Elite clients. Remote workers potentially access admin clients for both of these applications.

Remote workers do not need to log in to an Enterprise VPN to access the Avaya Workspaces for Call Center Elite applications.

Example of remote workers accessing Avaya Workspaces

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

For example, https://<*AvayaWorkspacesforEliteCluster PublicFQDN*/services/UnifiedAgentController/workspaces/#/login.

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

- External firewall allows the requests from remote workers through to the reverse proxy.
- Reverse proxy already has the configuration information set up to allow the requests to be processed securely. After checking the validity of the requests, the requests are forwarded to an internal IP address and port destination on the internal firewall.
- For any Avaya Workspaces for Call Center Elite solution, the reverse proxy has NAT entries for the different Avaya Workspaces for Call Center Elite servers.

Chapter 9: Deploy Web Voice and Web Video for remote workers

Overview

Avaya Workspaces for Call Center Elite provides Web Voice and Web Video configurations for remote workers. Based on your requirements, you can choose from the following configurations and complete all tasks:

- Avaya Workspaces for Call Center Elite with Avaya WebRTC Connect agents.

  With this configuration, WebRTC Connect agents can answer PSTN voice calls.

- Avaya Workspaces for Call Center Elite with web and mobile voice calls.

  With this configuration, phone-enabled agents can answer web and mobile voice calls that customers make through web and mobile devices on the public internet.

- Avaya Workspaces for Call Center Elite with web and mobile video calls and WebRTC Connect agents.

  With this configuration, WebRTC Connect agents can answer web and mobile video calls.

Important:

- Before doing any of these configurations, you must deploy the Elite voice solution.
- WebRTC Connect agents do not support the Auto answer feature. Therefore, do not configure WebRTC Connect agents to use this feature.

Checklist for configuring Avaya Workspaces for Call Center Elite with remote Avaya WebRTC Connect agents

Use the following checklist to configure Avaya Workspaces for Call Center Elite with remote WebRTC Connect agents so that the agents can answer PSTN Voice, Web Voice, and Web Video calls:

No.	Task	Description	✔
1	Install and configure Avaya Aura® Device Services, Avaya Aura® Media Server, and Avaya Aura® Web Gateway.	See the following: • Avaya Aura Device Services deployment on page 29. • Avaya Aura Media Server deployment on page 35. • Avaya Aura Web Gateway deployment and configuration on page 46.	
2	Configure authorization on Avaya Aura® Web Gateway.	See Avaya Aura Web Gateway authorization on page 52.	
3	Create Web Voice and Web Video agents that can use media in browsers.	See Creating a user in Avaya Control Manager on page 62.	
4	Install and configure Avaya Aura® Session Border Controller to enable customer PSTN Voice, Web Voice, and Web Video calls from the public internet.	See Install and configure Avaya Aura® Session Border Controller on page 72. See Deploying Identity Certificate on page 74.	
5	Install and configure Avaya Aura® Media Server.	See Install and configure Avaya Aura Media Server for Avaya Aura Web Gateway on page 36.	
6	Configuring the Javascript web reference client and making Web Voice and Web Video calls for testing and validation.	See Configuring the Javascript reference client and making a call on page 67.	

Install and configure Avaya Aura® Session Border Controller

Avaya Workspaces for Call Center Elite requires Avaya Aura® Session Border Controller to enable calls from the public internet. Therefore, you must install Avaya Aura® Session Border Controller as a part of your solution. For information about how to install Avaya Aura® Session Border Controller, see *Deploying Avaya Session Border Controller on a Hardware Platform*.

Checklist for installing and configuring Session Border Controller for remote worker

Use the following checklist to install and configure Session Border Controller for remote worker:

No.	Task	Description	✔
1	Configure Avaya Aura® Session Border Controller networks	See Configuring Avaya Aura Session Border Controller networks on page 73.	
2	Create a reverse proxy policy	See Creating a reverse proxy policy on page 73.	
3	Create the common client certificate	See Creating the common client certificate on page 75.	
4	Create the common server certificate	See Creating the common server certificate on page 76.	
5	Create a client profile for the Avaya Aura® Web Gateway reverse proxy	See Creating a client profile for the Avaya Aura Web Gateway reverse proxy on page 77.	
6	Create a server profile for the Avaya Aura® Web Gateway reverse proxy	See Creating a server profile for the Avaya Aura Web Gateway reverse proxy on page 77.	
7	Configure reverse proxy relay services	See Configure reverse proxy relay services on page 108.	
8	Configure Avaya WebRTC Connect client side TURN	See Configure Avaya WebRTC Connect client side TURN on page 114.	
9	Configure the trunk on Session Border Controller for PSTN customer calls	See Configure the trunk on Session Border Controller for PSTN customer calls on page 117.	
10	Configure TLS client and server profiles	See Configure TLS client and server profile on page 119.	

Configure reverse proxy relay services

For each server/cluster:port combination, you must configure a reverse proxy relay service. For multiple servers using the same port, such as 443, Avaya Aura® Session Border Controller directs the requests to the appropriate back-end server/cluster based on the URL in the request.

Configuring a relay service for Avaya Workspaces for Call Center Elite AuthorizationService

About this task

Use this procedure to configure a relay service for Avaya Workspaces for Call Center Elite AuthorizationService.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.

3. On the Reverse Proxy tab, click **Add**.

   The Add Reverse Proxy Profile page opens.

4. In the **Service Name** field, type the reverse proxy profile name.

   For example, Elite_AuthService.

5. Select the **Enabled** check box.
6. In the **Listen IP** field, select the B1 external network and select the B1 IP address used for the relay.
7. In the **Listen Port** field, type the Avaya Workspaces for Call Center Elite AuthorizationService port number as 9443.
8. In the **Listen Protocol** field, click HTTPS.
9. In the **Listen TLS Profile** field, select the server profile associated with the B1 interface.
10. Leave the **Listen Domain** field blank.
11. In the **Connect IP** field, select the internal A1 network and select the A1 interface IP address used for the relay.
12. In the **Server Protocol** field, click HTTPS.
13. In the **Server TLS Profile** field, select the client profile you create for the internal A1 interface.
14. In the **Reverse Proxy Policy Profile** field, select the default reverse proxy policy profile.
15. In the **Server Addresses** field, type *<Avaya Workspaces for Call Center Elite Cluster IP/FQDN>*:*9443*.

    <Avaya Workspaces for Call Center Elite Cluster IP/FQDN> is the internal firewall IP address of the cluster that hosts the UnifiedAgentController service.

16. In the **Whitelisted URL** field type `/services/AuthorizationService`.
17. Click **Finish**.
18. If you get the `specified port overlaps with range (9000-9999) use some different port` error, in the navigation pane, click **Network & Flows** > **Advanced Options** > **Port Ranges**.
19. Change the **Listen Port Range** to 9000-9400.
20. Repeat Steps 2 to 17.

Configuring the relay service for token-generation-service for Avaya Aura® Web Gateway

Before you begin

Create a reverse proxy policy through the EMS web interface, ensuring that the **Allow Web Socket** field for the reverse proxy policy is set to `Y`.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.
3. On the Reverse Proxy tab, click **Add**.

   The Add Reverse Proxy Profile page opens.
4. In the **Service Name** field, type the reverse proxy profile name.
5. Select the **Enabled** check box.
6. In the **Listen IP** field, click the external IP address of Session Border Controller.
7. In the **Listen Port** field, type the port number as 443.
8. In the **Listen Protocol** field, click HTTP/HTTPS.
9. In the **Listen TLS Profile** field, click the relevant TLS Profile.
10. In the **Server Protocol** field, click HTTP/HTTPS.
11. In the **Connect IP** field, click the internal IP address of Session Border Controller.
12. In the **Reverse Proxy Policy Profile** field, click the reverse proxy policy that you create.
13. In the **Server Addresses** field, type *<Avaya Aura Web Gateway_FQDN>*:*<port number>*.

    Use the FQDN based on what you use in the SAN name when creating the TLS certificate.

    The default port number on Avaya Aura® Web Gateway is 443. The value of *<port number>* must be the same as the port number configured in the **Front-end port** field on the HTTP Reverse Proxy page in Avaya Aura® Web Gateway.

    To go to the **HTTP Reverse Proxy** page, you must log on to the Avaya Aura® Web Gateway administration portal and click **External Access** > **HTTP Reverse Proxy**.
14. In the **Whitelisted URL** field, type `/token-generation-service/`.
15. Click **Finish**.

Configuring the relay service for Avaya Aura® Web Gateway for the external remote access

Before you begin

Create a reverse proxy policy through the EMS web interface, ensuring that the **Allow Web Socket** field for the reverse proxy policy is set to `Y`.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.

3. On the Reverse Proxy tab, click **Add**.

   The Add Reverse Proxy Profile page opens.
4. In the **Service Name** field, type the reverse proxy profile name.
5. Select the **Enabled** check box.
6. In the **Listen IP** field, click the external IP address of Session Border Controller.
7. In the **Listen Port** field, type the port number as 443.
8. In the **Listen Protocol** field, click HTTP/HTTPS.
9. In the **Listen TLS Profile** field, click the relevant TLS Profile.
10. In the **Server Protocol** field, click HTTP/HTTPS.
11. In the **Connect IP** field, click the internal IP address of Session Border Controller.
12. In the **Reverse Proxy Policy Profile** field, click the reverse proxy policy that you create.
13. In the **Server Addresses** field, type *<Avaya Aura Web Gateway_FQDN>*:*<port number>*.

    Use the FQDN based on what you use in the SAN name when creating the TLS certificate.

    The default port number on Avaya Aura® Web Gateway is 8444. The value of *<port number>* must be the same as the port number configured in the **Front-end port for external access** field on the HTTP Reverse Proxy page in Avaya Aura® Web Gateway on **Enable port for external access**.

    To go to the **HTTP Reverse Proxy** page, you must log on to the Avaya Aura® Web Gateway administration portal and click **External Access** > **HTTP Reverse Proxy**.
14. In the **Whitelisted URL** field, type `/csa/`.
15. Click **Finish**.

Configuring a relay service for Avaya Workspaces for Call Center Elite port 443

About this task

Use this procedure to configure a relay service for Avaya Workspaces for Call Center Elite port 443.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.
3. On the Reverse Proxy tab, click **Add**.

   The Add Reverse Proxy Profile page opens.
4. In the **Service Name** field, type the reverse proxy profile name.

For example, Elite_Relay.

5. Select the **Enabled** check box.
6. In the **Listen IP** field, select the B1 external network and select the B1 IP address used for the relay.
7. In the **Listen Port** field, type the Avaya Workspaces for Call Center Elite secure port number 443.
8. In the **Listen Protocol** field, click HTTPS.
9. In the **Listen TLS Profile** field, select the server profile associated with the B1 interface.
10. Leave the **Listen Domain** field blank.
11. In the **Connect IP** field, select the internal A1 network and select the A1 interface IP address used for the relay.
12. In the **Server Protocol** field, click HTTPS.
13. In the **Server TLS Profile** field, select the client profile you create for the internal A1 interface.
14. In the **Reverse Proxy Policy Profile** field, select the reverse proxy policy profile with WebSockets enabled.
15. In the **Server Addresses** and **Whitelisted URL** fields, type the address:port and URL combinations that are required for all applicable Avaya Workspaces for Call Center Elite servers/clusters. The Server Address is the IP address on the internal firewall that is allocated to each server/cluster.
16. Click **Finish**.

Configure the reverse proxy for Web Voice and Web Video remote workers

The reverse proxy determines which URL requests must be allowed and how the requests must flow into the enterprise applications. They also determine the reverse communications to remote workers.

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

The following table shows a sample whitelist configuration:

Cluster/Server	Whitelist URL in Request	Reverse Proxy Listen IP	Listen Port	Internal Firewall Destination IP	Internal Firewall Port
Avaya Workspaces for Call Center Elite Cluster 1	/services/CustomerManagement/				

Table continues…

Cluster/Server	Whitelist URL in Request	Reverse Proxy Listen IP	Listen Port	Internal Firewall Destination IP	Internal Firewall Port
Avaya Workspaces for Call Center Elite Cluster 1	/services/ OCPDataServices/				
Avaya Workspaces for Call Center Elite Cluster 1	/services/ CustomerJourneyService/				
Avaya Workspaces for Call Center Elite Cluster 2	/services/ UnifiedAgentController/				
Avaya Workspaces for Call Center Elite Cluster 2	/services/ Broadcast-UnifiedAgentController/				
Avaya Workspaces for Call Center Elite Cluster 1	/services/ AgentControllerService/				
Avaya Workspaces for Call Center Elite Cluster 1	/services/ CustomerControllerService/				
Avaya Workspaces for Call Center Elite Cluster 2	/services/ CoBrowse/				
Avaya Aura® Device Services	/acs/				
Avaya Aura® Device Services	/notification/				
Avaya Workspaces for Call Center Elite Cluster 2	/services/ AuthorizationService				

A remote worker who requests a destination containing an internal URL in the HTTPS request, such as /services/CustomerManagement/, gets forwarded to a preconfigured IP address and port on the internal firewall for that URL. The internal firewall uses its own rule (NAT) to allow or deny this request into the final internal destination component in Avaya Workspaces for Call Center Elite.

Note:

Reverse proxy relays requires you to enable WebSockets on the proxy connection for Avaya Workspaces for Call Center Elite Cluster 2 (UnifiedAgentController).

Configure Avaya WebRTC Connect client side TURN

Avaya Workspaces for Call Center Elite supports both client side TURN and server side TURN for WebRTC Connect calls from the public internet. Avaya recommends the use of client side TURN unless you must use server side TURN.

Adding a TURN/STUN service for Avaya WebRTC Connect clients

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the navigation pane, click **DMZ Services** > **TURN/STUN Service** > **TURN/STUN Profiles**.
3. On the TURN/STUN Profiles tab, click **Add**.
4. In the **Profile Name** field, type an appropriate profile name.
5. In the **UDP Listen Port** field, type `3478`.
6. In the **TCP/TLS Listen Port** field, type `443`.
7. In the **TLS Server Profile** field, select the profile created in Creating a server profile for the TLS TURN relay on page 80.
8. In the **Media Relay Port Range** field, type a value between 50000 to 55000.
9. In the **Authentication** field, enable the authentication.
10. In the **Client Authentication** field, enable the authentication.
11. In the **Realm** field, specify the SIP domain.
12. In the **UDP Relay** field, enable the UDP relay.
13. Click **Finish**.
14. On the TURN Relay tab, click **Add**.
15. In the **Listen IP** field, enter the external interface IP configured on Avaya Aura® Session Border Controller that external clients use.
16. In the **Media Relay IP** field, enter the internal IP configured on Avaya Aura® Session Border Controller that Avaya Aura® Web Gateway and Avaya Aura® Media Server use for media.
17. Keep the **Service FQDN** field blank.
18. In the **TURN/STUN Profile** field, select the TURN/STUN profile that you created.
19. Click **Finish**.

Enabling Avaya WebRTC Connect Client Side TURN on Web Gateway

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. Log on to Avaya Aura® Web Gateway administration portal with your administrator credentials.
3. On the Avaya Aura® Web Gateway administration portal, click **External Access** > **Session Border Controller** .
4. Select the **Enable TURN in WebRTC Client** check box.
5. Click **Save**.

Adding the STUN server configuration to Avaya Aura® Web Gateway

Procedure

1. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. Log on to Avaya Aura® Web Gateway administration portal with your administrator credentials.
3. On the Avaya Aura® Web Gateway administration portal, click **External Access** > **STUN Servers** .
4. Click **Add**.
5. In the **Address** field, enter the address of the STUN server.

   Based on the network configuration of Avaya Aura® Session Border Controller, this address can be either of the following:

   - The external IP that you used when configuring the TURN Relay in Avaya Aura® Session Border Controller
   - The address on the external firewall that receives media and directs it to the Avaya Aura® Session Border Controller Relay IP address.

6. In the **Port** field, type `3478`.
7. Click **Save**.
8. To set the STUN priority, select the newly added STUN server and click **Add** to add it to the list of Assigned STUN Servers.
9. Click **Save**.

Enabling the 8444 port on Avaya Aura® Web Gateway

About this task

Use this procedure to enable the 8444 port on Avaya Aura® Web Gateway to properly handle the media for external users. All requests from remote clients such as customer reference client or remote Avaya WebRTC Connect agents, must go to the remote access port 8444 and not to 443. It specifies that Avaya Aura® Web Gateway can identify remote and local clients.

Procedure

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

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. On the Avaya Aura® Web Gateway administration portal, click **External Access** > **HTTP Reverse Proxy**.
3. Select the **Enable port for remote access** check box.
4. In the **Front-end port for remote access** field, enter the port number 8444.

   Avaya Aura® Web Gateway uses this port number to distinguish between clients on the internal network and external clients on the internet. Internal clients use the standard 443 port whereas external clients such as Browsers, Android, and iOS use the 8444 port to access Avaya Aura® Web Gateway. Based on the port number, Avaya Aura® Web Gateway sets the media paths.

5. Click **Save**.

Changing the load balancing configuration in Session Border Controller

About this task

Use this procedure to fix the Avaya Aura® Web Gateway load monitoring by changing the load balancing configuration in Session Border Controller.

Procedure

1. Log in to the Avaya Aura® Session Border Controller web administration portal.
2. In the navigation pane, click **Device Specific Settings** > **Advanced Options** > **Load Monitoring**.
3. On the Edit Load Balancer Config dialog box, in the **Transport** field, select `TCP`.
4. In the **Service Type** field, select `Turn`.

Configuring the HTTP port and protocol of Avaya Aura® Session Border Controller

About this task

Use this procedure to configure the HTTP port and protocol of Avaya Aura® Session Border Controller to match the TCP transport type configured on Session Border Controller.

Procedure

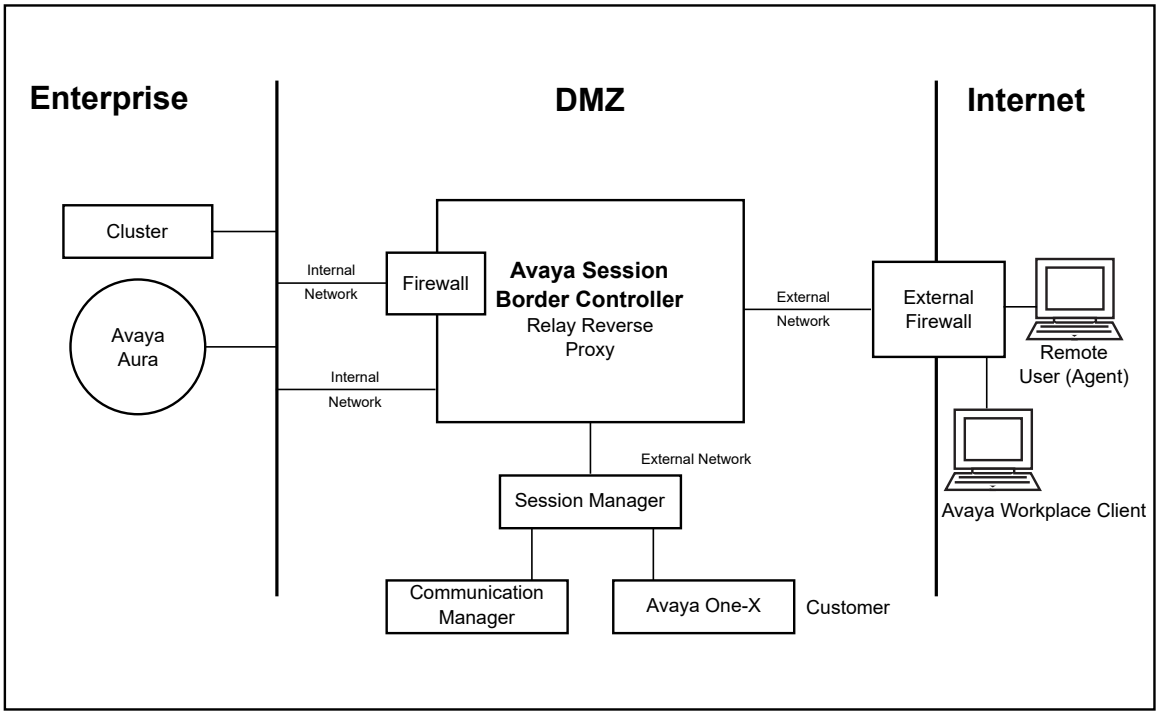
1. In your web browser, enter the following URL to log on to Avaya Aura® Web Gateway administration portal:

   `https://<Avaya Aura Web Gateway_FQDN>:8445/admin`

2. On the Avaya Aura® Web Gateway administration portal, click **External Access** > **Session Border Controller**.
3. Select the Session Border Controller and click **Edit**.
4. In the **HTTP Port** field, type `80`.
5. In the **HTTP Protocol** field, select `http`.
6. Click **Save**

Configure the trunk on Session Border Controller for PSTN customer calls

The following diagram depicts the architecture for PSTN call to remote users:



Configuring Avaya Aura® Session Border Controller networks for PSTN calls

About this task

Avaya Workspaces for Call Center Elite exclusively supports on-premise Avaya Workspaces agents. It specifies that the agents must be on site, behind the enterprise firewalls to log on to Avaya Workspaces and accept contacts.

This procedure has a reference configuration where the PSTN customers make calls through the Session Border Controller trunk. Session Border Controller can be configured to allow external agents to access Avaya Workspaces for Call Center Elite from a remote location with Internet access, so that PSTN trunk calls are routed to remote location agent through the Session Border Controller trunk.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Specific Settings** > **Network Management** > **Interfaces**.
3. On the Interfaces page, enable the following interfaces:
   - A1 internal interface
   - B1 external interface
4. On the Networks tab, configure the following networks:
   - A1 internal network
   - B1 external network
5. For external PSTN trunk access, assign the IP addresses to each network as follows:

   The external IP address:

   - One IP address for the external network.

   The internal IP address:

   - One IP address for the internal network.

Creating a routing profile for customer Session Manager entity on Session Border Controller

About this task

Use this procedure to create a routing profile that creates a trunk between Session Border Controller and customer Session Manager.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Configuration Profiles** > **Routing**.
3. In the content pane, click **Add**.

4. In the **Profile Name** field, enter a name for the customer Session Manager trunk.

   For example, SM2_Trunk.

5. Set the **Time of Day** field to `default`.
6. Set the **Load Balancing** field to `Priority`.
7. Set the **Next Hop Address** field to customer Session Manager.
8. Set the **TLS** port to `5061`.
9. Click **Finish**.

Creating a topology hiding profile

About this task

Use this procedure to create a topology hiding between the agent and customer domains on Session Border Controller.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Configuration Profiles** > **Topology Hiding**.
3. In the content pane, click **Add**.
4. In the **Profile Name** field, enter a name for the customer domain trunk.

   For example, wslab.com.

5. Enter appropriate details in the **From**, **To**, **Request Line**, and **SDP Headers** fields.
6. Click **Finish**.

Configure TLS client and server profile

The Session Border Controller PSTN trunk requires a TLS client profile and a TLS server profile. The client profile is for the interface facing towards the internal Avaya Workspaces for Call Center Elite servers/clusters and the server profile is for the interface facing towards the Internet.

Creating a TLS client profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management** > **Client Profiles**.
3. On the Client Profiles page, click **Add**.
4. In the **Profile Name** field, type the name of the profile.

   For example, client_sm247.

5. In the **Certificate** field, select a certificate corresponding to the internal interface IP address that acts as a **Connect IP** for SIP Trunk.

For this reference configuration, the certificate used has the Session Border Controller FQDN as the CN and included the FQDN and the A1 interface IP address in the Subject Alternate Name (SAN).

6. In the **Peer Certificate Authority** field, select the CA that is used to sign the identity certificates for the internal Avaya Workspaces for Call Center Elite servers/clusters.
7. In the **Verification Depth** field, type 1.
8. Keep other fields at default values.
9. Click **Next**.
10. Click **Finish**.

Creating a TLS server profile

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **TLS Management** > **Server Profiles**.
3. On the Server Profiles page, click **Add**.
4. In the **Profile Name** field, type the name of the profile.

   For example, Server_sm247.
5. In the **Certificate** field, select a certificate corresponding to the external interface IP that you need to specify in the **Listen IP** field for the SIP Trunk.

   For this reference configuration, the certificate used has the Session Border Controller FQDN as the CN and included the FQDN and the B1 interface IP address in the Subject Alternate Name (SAN).
6. In the **Peer Verification** field, click **None**.
7. Keep the default values in the other fields.
8. Click **Next**.
9. Click **Finish**.

Creating a SIP entity between the Session Border Controller external interface and customer Session Manager

About this task

Use this procedure to create a SIP entity between the Session Border Controller external interface and customer Session Manager on the customer System Manager.

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **SIP Entities**.
2. On the SIP Entities page, click **New**.
3. In the **Name** field, enter a name for the SIP entity.

4. In the **FQDN or IP Address** field, enter the FQDN or IP address of the SIP entity.
5. In the **Type** field, select **SIP Trunk**.
6. Click **Commit**.

Creating a routing policy for the Session Border Controller external interface SIP entity link

About this task

A routing policy defines how Session Manager routes calls between SIP network elements. Session Manager uses the data configured in the routing policy to find the best match against the number or address of the called party.

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **Routing Policies**.
2. Verify the routing policy for the Experience Portal Media Processing Platform entity link.

   If the routing policy does not exist, complete the remainder of this procedure.
3. On the Routing Policies page, click **New**.
4. In the **Name** field, enter a name for the routing policy.

   For example, SBC_Trunk.
5. In the **Retries** field, enter the number of retries.
6. In the SIP Entity as Destination section, click **Select**.
7. Select the Session Border Controller external interface SIP entity as the destination for the routing policy and click **Select**.
8. Click **Commit**.

Creating a SIP entity between the Session Border Controller internal interface and agent Session Manager

About this task

Use this procedure to create a SIP entity between the Session Border Controller internal interface and agent Session Manager on the agent System Manager.

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **SIP Entities**.
2. On the SIP Entities page, click **New**.
3. In the **Name** field, enter a name for the SIP entity.
4. In the **FQDN or IP Address** field, enter the FQDN or IP address of the SIP entity.
5. In the **Type** field, select **SIP Trunk**.
6. Click **Commit**.

Creating a routing policy for the Session Border Controller internal interface SIP entity link

About this task

A routing policy defines how Session Manager routes calls between SIP network elements. Session Manager uses the data configured in the routing policy to find the best match against the number or address of the called party.

Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **Routing Policies**.
2. Verify the routing policy for the Experience Portal Media Processing Platform entity link.

   If the routing policy does not exist, complete the remainder of this procedure.
3. On the Routing Policies page, click **New**.
4. In the **Name** field, enter a name for the routing policy.

   For example, SBC_Trunk.
5. In the **Retries** field, enter the number of retries.
6. In the SIP Entity as Destination section, click **Select**.
7. Select the Session Border Controller internal interface SIP entity as the destination for the routing policy and click **Select**.
8. Click **Commit**.

Chapter 10: Configure Avaya Session Border Controller for external mobile client access

Overview

Avaya Aura® Session Border Controller supports incoming calls from WebRTC-enabled web browsers to an internal Avaya Aura® network with SIP at the core. For example, a consumer can call an Avaya Aura® network by using a WebRTC-enabled browser from an external network.

This chapter describes the Avaya Aura® Session Border Controller configuration process for external mobile client access.

Configuring the TLS server profile for Avaya Aura® Session Border Controller external communication

About this task

Avaya Aura® Session Border Controller uses a TLS server profile to process an incoming connection over TLS from a remote client.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. In the navigation pane, click **TLS Management** > **Server Profiles**.
4. On the Server Profiles page, click **Add**.
5. In the **Profile Name** field, type the name of the profile.
6. In the **Certificate** field, select the certificate for external communication.
7. In the **SNI Options** field, click **None**.
8. In the **Peer Verification** field, click **None**.
9. Leave the **Extended Hostname Verification** check box cleared.

10. In the **Renegotiation Time** field, set the value to `0`.
11. In the **Renegotiation Byte Count** field, set the value to `0`.
12. In the **Version of handshake options** field, select `TLS 1.2`.
13. In the **Ciphers** field, set the value to `Default`.

    For more information, see *Administering Avaya Session Border Controller*.
14. Click **Finish**.

Configuring the TLS server profile for Avaya Aura® Session Border Controller media tunneling

About this task

With a TLS profile, Avaya Aura® Session Border Controller can control parameters when it performs a TLS handshake with a remote entity. HTTPS media tunneling requires its own TLS server profile. Session Border Controller supports media tunneling for sign-in and guest users. This configuration is required only for external mobile calls that are inbound towards Session Border Controller.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. In the navigation pane, click **TLS Management** > **Server Profiles**.
4. On the Server Profiles page, click **Add**.
5. In the **Profile Name** field, type the name of the profile.
6. In the **Certificate** field, select the certificate that the TLS server profile uses for external communication.
7. In the **SNI Options** field, click **None**.
8. In the **Peer Verification** field, click **Optional**.
9. Leave the **Peer Certificate Authorities** field empty.
10. Leave the **Peer Certificate Revocation Lists** field empty.
11. In the **Verification Depth** field, set the value to `1`.
12. Leave the **Extended Hostname Verification** check box cleared.
13. In the **Renegotiation Time** field, set the value to `0`.
14. In the **Renegotiation Byte Count** field, set the value to `0`.
15. In the **Version of handshake options** field, select `TLS 1.2`.

16. In the **Ciphers** field, set the value to `Default`.

    For more information, see *Administering Avaya Session Border Controller*.

17. Click **Finish**.

Configuring the TLS client profile on Avaya Aura® Session Border Controller

About this task

A TLS client profile is used when Avaya Aura® Session Border Controller starts an outgoing connection towards a remote entity over TLS.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. In the navigation pane, click **TLS Management** > **Server Profiles**.
4. On the Server Profiles page, click **Add**.
5. In the **Profile Name** field, type the name of the profile.
6. In the **Certificate** field, select the certificate for internal communication.
7. In the **SNI Options** field, click **None**.
8. In the **Peer Verification** field, click **Required**.
9. In the **Peer Certificate Authorities** field, select the System Manager Certificate Authority certificate.
10. Leave the **Peer Certificate Revocation Lists** field empty.
11. In the **Verification Depth** field, set the value to `1`.
12. Leave the **Extended Hostname Verification** check box cleared.
13. In the **Renegotiation Time** field, set the value to `0`.
14. In the **Renegotiation Byte Count** field, set the value to `0`.
15. In the **Version of handshake options** field, select `TLS 1.2`.
16. In the **Ciphers** field, set the value to `Default`.

    For more information, see *Administering Avaya Session Border Controller*.

17. Click **Finish**.

Configuring Avaya Aura® Session Border Controller network interfaces

About this task

Use this procedure to configure Avaya Aura® Session Border Controller network interfaces.

For detailed information about system configuration, server and network configuration, device configuration, and WebRTC-enabled call processing, see *Administering Avaya Session Border Controller*.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. In the navigation pane, click **Network & Flows** > **Network Management** > **Networks**.
4. In addition to the management interface configured during Session Border Controller installation, configure the following interfaces:
   - A1 internal interface with at least two IP addresses associated to it.
   - B1 external IP addresses with at least two IP addresses associated to it.

Configuring the Avaya Aura® Session Border Controller signaling interface

About this task

Use this procedure to configure the external and internal signaling interfaces for your deployment.

For detailed information about signaling interface configuration, see *Administering Avaya Session Border Controller*.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. To configure the external signaling interface, in the navigation pane, click **Network & Flows** > **Signaling Interface**.
4. Click **Add**.
5. In the **Name** field, enter the name for the external signaling interface (B1).
6. In the **IP Address** field, enter the network name and the IP address of the Session Border Controller used by SIP signaling messages traversing the network.

   The network name is identified by the interface name and VLAN tag.

7. Leave the **TCP Port** field blank.
8. Leave the **UDP Port** field blank for a non-tunneled mode.
9. In the **TLS Port** field, type `5061`.
10. In the **TLS Profile** field, select the previously configured TLS profile.
11. Keep the **Enable Shared Control** check box cleared.
12. Leave the **Shared Control Port** field blank.
13. Click **Finish**.
14. To configure the internal signaling interface, in the navigation pane, click **Network & Flows** > **Signaling Interface**.
15. Click **Add**.
16. In the **Name** field, enter the name for the internal signaling interface (A1).
17. In the **IP Address** field, enter the network name and the IP address of the Session Border Controller used by SIP signaling messages traversing the network.

    The network name is identified by the interface name and VLAN tag.
18. Leave the **TCP Port** field blank.
19. Leave the **UDP Port** field blank for a non-tunneled mode.
20. In the **TLS Port** field, type `5061`.
21. In the **TLS Profile** field, select the previously configured TLS profile.
22. Keep the **Enable Shared Control** check box cleared.
23. Leave the **Shared Control Port** field blank.
24. Click **Finish**.

Configuring the Avaya Aura® Session Border Controller media interface for external mobile client

About this task

Use this procedure to configure the media interface for external mobile client.

For detailed information about media tunneling, media interface, media video, and end point policy groups, see *Administering Avaya Session Border Controller*.

Before you begin

To configure the media interface, you must use the same listen IP interface that is selected for STUN/TURN. Therefore, ensure that you take a note of the listen IP interface.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. In the navigation pane, click **Network & Flows** > **Advanced Options**.
4. On the Feature Control tab, select the **Media Tunneling** check box and click **Save**.
5. Click **Add**.
6. **Configure the external media interface**: In the navigation pane, click **Network & Flows** > **Media Interface**.
7. Click **Add** or clone an existing media rule.
8. In the **Name** field, enter the name for the external media interface.
9. In the **IP Address** field, enter the B1 IP address ensuring that you:
   - Do not use this IP address for any other interface bound to port 443 (HTTP tunneling configuration).
   - Do not use VLAN tag for media tunneled interface.
10. In the **Port Range** field, enter a range such as `35000-40000`.
11. In the **TLS Profile** field, select the TLS server profile for the media interface that you created. For self-signed certificates on the client, use the TLS server profile created for the external media interface.

    If media tunneling is disabled, keep the value `None`.
12. In the **Buffer Size** field, select the buffer size from the list containing values from 400 to 1000 in KB.
13. Click **Finish**.
14. **Configure the internal media interface**: In the navigation pane, click **Network & Flows** > **Media Interface**.
15. Click **Add** or clone an existing media rule.
16. In the **Name** field, enter the name for the internal media interface.
17. In the **IP Address** field, enter the A1 IP address for media tunneling.
18. In the **Port Range** field, enter a range such as `35000-40000`.
19. In the **TLS Profile** field, select the TLS server profile for the media interface that you created. For self-signed certificates on the client, use the TLS server profile created for the internal media interface.
20. In the **Buffer Size** field, select the buffer size from the list containing values from 400 to 1000 in KB.
21. Click **Finish**.
22. **Enable video media**: In the navigation pane, click **Domain Policies** > **Application Rules**.

23. Clone an existing rule or add a new rule.
24. Enable **In/Out Audio/Video** application types.
25. Configure **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** fields.
26. **Configure media encryption and enable BFCP/FECC**: In the navigation pane, click **Domain Policies** > **Media Rules**.
27. Clone an existing rule or add a new rule.
28. On the Encryption tab, in the Miscellaneous section, select the **Capability Negotiation** check box.
29. On the Advanced tab, select the **BFCP Enabled** and **FECC Enabled** check boxes.
30. **Configure the policy group with the newly created application and media rules**: In the navigation pane, click **Domain Policies** > **End Point Policy Groups**.
31. Clone an existing policy group or add a new policy group.
32. **Disable interworking when using HTTP tunneling**: In the navigation pane, click **Domain Policies** > **Media Rules** > **Encryption**.
33. Clear the **Interworking** check box.

Configuring Avaya Aura® Session Border Controller load monitoring for external mobile access

About this task

Use this procedure to configure load monitoring for external mobile access.

For detailed information about load monitoring, see *Administering Avaya Session Border Controller*.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. In the navigation pane, click **Network & Flows** > **Load Monitoring** > **Advanced Options**.
4. Click **Add** to create a new load balancer profile.
5. In the **Load Balancer Type** field, select `INTERNAL`.

   Load Balancer on the A1 side of the network. Avaya Aura® Web Gateway does the load balancing towards the internal side. All HTTP requests sent out for dialing use the internal load balancer logic to identify the appropriate Session Border Controller.
6. In the **Transport** field, select the load balancer protocol.

7. In the **Listen IP** field, select the internal interface (A1) IP address.

   It can be a separate IP address.
8. In the **Service Type** field, select `TURN`.

Configuring Avaya Aura® Session Border Controller server flows for external mobile calls

About this task

Use this procedure to configure the server flows for external mobile calls.

For detailed information about server flows, see *Administering Avaya Session Border Controller*.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. **Create an interworking profile or update an existing profile**: In the navigation pane, click **Configuration Profiles** > **Server Interworking**.
4. Click **Add** to create a new profile.
5. For a new profile, set all options as default.
6. In the Advanced Options section, in the **Has Remote SBC** field, select `No`.
7. In the **Extensions** field, select the correct profile.

   This configuration directs the Session Border Controller security device to use the functionality specific to different environments.
8. Click **Finish**.
9. **Add a configuration for Session Manager**: In the navigation pane, click **Services** > **SIP Servers**.
10. Click **Add**.
11. In the **Server Type** field, select `Call Server`.
12. Leave the **SIP domain** field blank.
13. In the **TLS Client Profile** field, select the previously created client profile if TLS port is specified.

    Add the Session Manager IP or FQDN with port and protocol specified (TCP and/or TLS).
14. In the Advanced Options section, select the **Enable Grooming** check box, and then select the previously created interworking profile.
15. Leave the other settings with their default values.

16. Click **Finish**.
17. **Add a flow for Session Manager**: In the navigation pane, click **Network & Flows** > **End Point Flows** > **Server Flows**.
18. Click **Add**.
19. In the **Flow Name** field, enter a name such as `SM_Flow`.
20. In the **SIP Server Profile** field, select the configuration that you previously created for the SIP Server profile for Session Manager.
21. In the **Received Interface** field, select the internal interface (A1).
22. In the **Signaling Interface** field, select the internal interface (A1).
23. In the **Media Interface** field, select the internal interface (A1).
24. In the **Endpoint Policy Group** field, select the appropriate option.
25. Leave the other settings with their default values.
26. Click **Finish**.
27. **Add a configuration for the Avaya Aura® Web Gateway server**: In the navigation pane, click **Services** > **SIP Servers**.
28. Click **Add**.
29. In the **Server Type** field, select `Trunk Server`.
30. Leave the **SIP domain** field blank.
31. In the **TLS Client Profile** field, select the previously created Avaya Aura® Web Gateway client profile if TLS port is specified.

    Add the Avaya Aura® Web Gateway IP or FQDN with port and protocol specified (TCP and/or TLS). Add all cluster nodes.
32. In the Advanced Options section, select the **Enable Grooming** check box, and then select the previously created interworking profile.
33. Leave the other settings with their default values.
34. Click **Finish**.
35. **Add a flow for the Avaya Aura® Web Gateway server**: In the navigation pane, click **Network & Flows** > **End Point Flows** > **Server Flows**.
36. Click **Add**.
37. In the **Flow Name** field, enter a name such as `AAWGFlow`.
38. In the **SIP Server Profile** field, select the configuration that you previously created for Avaya Aura® Web Gateway.
39. In the **Received Interface** field, select the internal interface (A1).
40. In the **Signaling Interface** field, select the internal interface (A1).
41. In the **Media Interface** field, select the external interface (B1).

42. In the **Endpoint Policy Group** field, select the appropriate option.
43. Leave the other settings with their default values.
44. Click **Finish**.

Configuring Avaya Aura® Session Border Controller STUN TURN server for external mobile calls

About this task

Use this procedure to configure the STUN TURN server for external mobile calls.

For detailed information about WebRTC Connect-enabled call processing, see *Administering Avaya Session Border Controller*.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the **Device** drop-down list, select ASBCE.
3. In the navigation pane, click **DMZ Services** > **TURN/STUN Service** > **TURN/STUN Profiles**.
4. On the TURN/STUN Profiles tab, click **Add**.
5. In the **Profile Name** field, type an appropriate name.
6. In the **UDP Listen Port** field, type `3478`.
7. In the **Media Relay Port Range** field, type the port range.
8. Select the **Media Learning** check box only for deployments with TURN on Avaya Media Server or MCU.

   Clear this check box for TURN/STUN profile deployment on browser.
9. Click **Finish**.
10. On the TURN Relay tab, click **Add**.
11. In the **Listen IP** field, enter the Listen IP of the TURN server.

    It shows the IP that you created in the TURN/ STUN Profiles tab for the Session Border Controller device.
12. In the **Media Relay IP** field, enter the media relay IP of the TURN server.

    It shows the IP that you created in the TURN/ STUN Profiles tab for the Session Border Controller device.
13. In the **Service FQDN** field, enter the Listen FQDN of the TURN server.
14. In the **TURN/STUN Profile** field, select the TURN/STUN profile that you created.

15. Click **Finish**.

Chapter 11: Configure Avaya Workplace

Overview

Avaya Workplace Client is a SIP based softphone application that provides users access to Avaya Aura® Unified Communications voice features in its simplest form. It can also provide users access to conferencing capabilities, video capabilities, collaboration and presence, directory features (AD/LDAP) and screen sharing.

Configuring Avaya Workplace Client for Windows

Before you begin

Install the following:

- Latest version of Avaya Workplace Client for Windows
- System Manager certificate

Procedure

1. Open Avaya Workplace Client for Windows.
2. Navigate to **Settings** > **Accounts**.
3. In the **Extension** field, enter the extension.
4. In the **Password** field, enter the password.
5. In the navigation pane, click **Services**.
6. In the **Services** field, select the `Phone Service`.
7. In the **Server Address** field, enter the SIP IP address of Session Manager.
8. In the **Server Port** field, enter the port number 5061 for TLS.
9. In the **Domain** field, enter the domain.
10. Click **DONE**.
11. Login using the extension and password.

Enabling the Button Module for agent login

Procedure

1. Navigate to the following location:

   `%USERPROFILE%>\AppData\Roaming\Avaya\Avaya IX Workplace`

2. Open the `configdata.xml` file in a text editor such as Notepad.
3. Edit the following values:

```
<EnableButtonModule locked="false" obscured="false">
<value>true</value>
</EnableButtonModule>



<agentConfiguration>
<agentServiceEnabled locked="false" obscured="false">
<value>true</value>
</agentServiceEnabled>
<autoLoginFlag locked="false" obscured="false">
<value>true</value>
</autoLoginFlag>
<configurableFeatureButtonsNumber locked="false" obscured="false">
<value xsi:nil="true" />
</configurableFeatureButtonsNumber>
<availableFeatureButtonList locked="false" obscured="false">
<values xsi:nil="true" />
</availableFeatureButtonList>
</agentConfiguration>
```

4. Restart the Avaya Workplace Client for Windows.
5. Click the **Button Module** () icon at the bottom-right corner.
6. On the Button Module screen, click **Login Customer**.
7. In the **Customer Service ID** and **Password** fields, enter the login credentials of the agent.
8. Click **LOGIN**.

Chapter 12: Troubleshooting the Avaya Aura® Web Gateway TestApp issues

Troubleshooting Error 401

Condition

Error 401 unauthorized.

Cause

The port number in the earlier release of Avaya Aura® Web Gateway was 8443, which is no longer valid for the latest release.

Solution

Change the port number to 8445.

Troubleshooting the activation issue

Condition

Unable to activate.

Cause

Session Manager might not be configured to use System Manager certificates.

Solution

Configure Session Manager to use System Manager certificates.

Chapter 13: Troubleshooting Avaya WebRTC Connect

Troubleshooting for Avaya WebRTC Connect agents

Failed to activate an agent

Solution

1. In the browser, do the following:
   a. Accept the certificates for the Avaya Aura® Device Services URL:

      `https://<Avaya Aura Device Services_FQDN>/acs/resources`

   b. Accept the certificates for the Avaya Aura® Web Gateway URL:

      `https://<Avaya Aura Web Gateway_FQDN>/csa/resources/tenants/default`

   c. Refresh the page and retry agent activation.
2. To accept the certificates, do the following:
   a. Clear the browser cache and repeat Step 1.
   b. **(Optional)** Restart the browser as a guest user and go to the Avaya Workspaces URL.
3. Go to the following URL for Avaya Aura® Device Services automatic configuration:

   `https://<Avaya Aura Device Services_FQDN>:8443/acs/resources/configurations`

   You can view an output similar to the following:

```
## File Generation Notes
## Avaya Dynamic Configuration Service does not recognize User-Agent -
SET SIPSECURE 0
SET SIPENABLED 1
SET SIPDOMAIN oceana.com
SET SIPUSERNAME 8832018
SET SIPHA1 b459b107705c7277cf936acb3b476d5c
SET ACSPORT 8843
SET ACSSECURE 1
SET ACSENABLED 1
SET ACSSSO 1
SET SIP_CONTROLLER_LIST 10.133.34.202:5061;transport=TLS
SET ACSSRVR 10.133.34.204
SET SIPPROXYSRVR 10.133.34.202
SET SIPPORT 5061
```

```
SET LOCKED_PREFERENCES "SIPSECURE,SIPENABLED,SIPDOMAIN,SIPUSERNAME,SIPl
SET OBSCURE_PREFERENCES ""
```

4. **(Optional)** If you do not receive an output with the user configuration details, do the following:
   a. Go to **Start** > **Administrative tools** > **Active Directory** and check if the email field is populated.
   b. **(Optional)** If the email field is empty, specify the user email in the `username@domain` format.
   c. Ensure that the user is added to the group that is used for publishing in Avaya Aura® Device Services.
   d. On the Avaya Aura® Device Services web interface, click **Server Connections** > **LDAP Configuration**.
   e. On the LDAP Configurations page, ensure that the **Role Filter** and **Role Attribute ID** fields are populated.
   f. In **User Role**, type the LDAP group name.

      For more information about the LDAP group name configuration, see *Administering Avaya Aura® Device Services*.
   g. On the Avaya Aura® Device Services web interface, click **Dynamic Configuration** > **Configuration** > **Group**.
   h. On the Group page, configure the following parameters:

      `COMM_ADDR_HANDLE_TYPE = Avaya SIP`

      `COMM_ADDR_HANDLE_LENGTH = <Length of your SIP Extensions>`
   i. Publish the LDAP group configuration.
5. Check the connection between Avaya Control Manager and UCAStoreService.
6. Check the CTI-Link from Communication Manager to the Application Enablement Services server.
7. Check whether as common certificate along with the Certificate Authority (CA) certificate is installed on the client machine.
8. Check whether Avaya Aura® Web Gateway and Avaya Aura® Device Services FQDNs are correctly configured in the UnifiedAgentController attributes.

Authentication failures

Solution

1. Check the connection between Avaya Aura® System Manager and LDAP server.
2. Check the LDAP synchronization on the User Management page in System Manager.
3. Check LDAP certificates on all Avaya Breeze® platform nodes.
4. Check authorization certificates update at the cluster level.
5. Ensure that a common certificate is installed on Avaya Breeze® platform nodes, Avaya Aura® Web Gateway, and Avaya Aura® Device Services.

6. Check whether the common certificates are expired.

Avaya Workspaces displays an error in registering the agent

Solution

1. Check the Avaya Aura® Device Services and LDAP connection on Avaya Aura® Device Services.
2. Check the Avaya Aura® Web Gateway and LDAP connection on Avaya Aura® Web Gateway.
3. Check whether a SIP handle is assigned to the System Manager user.
4. Check whether the LDAP users are assigned to the same group configured and published on Avaya Aura® Device Services.
5. Check whether the **Type of 3PCC Enabled** is set as `Avaya` on the Station page of the SIP station assigned to the Avaya Workspaces agent.

Avaya Workspaces displays the Provider not found error

Solution

1. Check the connection between the Call Server Connector (CSC) service and Application Enablement Services server.
2. Check the connection between Avaya Control Manager and UCAStoreService.
3. Check the CTI-Link from Communication Manager to the Application Enablement Services server.
4. Create a new agent in Avaya Control Manager.
5. Restart the Unified Agent Controller (UAC) cluster.
6. Redeploy the UAC cluster.

Cannot change agent states in Avaya Workspaces

Condition

Agent retains the Reconnecting state on Avaya Workspaces.

Solution

1. Close the existing TSAPI sessions on Application Enablement Services (AES).
2. After sessions are recreated, restart AES.
3. Reboot AES.
4. Ensure that the **Date/Time** value is the same on AES, CM, and nodes.
5. Check the CTI-Link from Communication Manager to the AES server, unlink the link, and add it again.
6. Check the connection between the Call Server Connector (CSC) service and AES server.
7. Restart the AES TSAPI and DMCC services.

8. Reboot the cluster.

Authorization error on Workspaces

Condition

Avaya Workspaces displays the following error:

```
Unable to contact the authentication server. Please try again, and if
the problem persists please contact your system administrator.
```

Solution

1. Add the AD certificates again on each node.
2. Restart the cluster.
3. Reinstall Authorization Service.

Unable to contact the authentication server on Workspaces

Solution

1. Ensure that the LDAP password is not reset.
2. On the System Manager web interface, click **Users** > **Directory Synchronization** and check the LDAP connection.
3. To Reinstall the LDAP certificate on the Session Manager and all the nodes, do the following:
    a. On the System Manager web interface, click **Services** > **Inventory** > **Manage Elements**.
    b. On the Manage Elements page, select the check box for one of the nodes of the proposed cluster.
    c. Click **More actions** > **Manage Trusted Certificates**.
    d. On the Manage Trusted Certificates page, click **Add**.
    e. On the Add Trusted Certificate page, do the following:
        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**.

Communication package error on Avaya Workspaces

Solution

1. Restart the Unified Agent Controller (UAC) cluster.
2. **(Optional)** If restarting the cluster does not solve the issue, redeploy the UAC cluster.

Error 404 on Workspaces

Solution

1. Go to **Logs of Authorization**.
2. Ensure that the log file shows the following error:

```
java.lang.IllegalArgumentException: Service AuthorizationService-3.7.0.0.370008
cannot be found on cluster
at
com.avaya.zephyr.platform.dao.AusServiceLevelTLSVersionDAO.getServiceLevelTLSVersi
onForMyCluster(AusServiceLevelTLSVersionDAO.java:228)
at
com.avaya.collaboration.ssl.util.SSLUtilityHelper.getClusterTLSVersion(SSLUtilityH
elper.java:61)
at
com.avaya.collaboration.ssl.util.SSLUtilityImpl.getClusterTLSVersion(SSLUtilityImp
l.java:405)
at
com.avaya.collaboration.ssl.util.SSLUtilityImpl.createSSLContext(SSLUtilityImpl.ja
va:85)
at
com.avaya.collaboration.ssl.util.SSLUtilityFactoryImpl.createSSLContext(SSLUtility
FactoryImpl.java:25)
at
com.avaya.collaboration.ssl.util.SSLUtilityFactory.createSSLContext(SSLUtilityFact
ory.java:104)
at
com.avaya.zephyr.services.production.AuthorizationService.startup.StartupServlet.i
nitializeHttpClient(StartupServlet.java:169)
at
com.avaya.zephyr.services.production.AuthorizationService.startup.StartupServlet.l
ambda$initializeHttpClient$0(StartupServlet.java:186)
at
com.avaya.zephyr.services.production.AuthorizationService.startup.StartupServlet$
$Lambda$50.0000000022C48410.run(Unknown Source)
at java.util.concurrent.Executors$RunnableAdapter.call(Executors.java:522)
at java.util.concurrent.FutureTask.run(FutureTask.java:277)
at
java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.access$201(Sc
heduledThreadPoolExecutor.java:191)
at
java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.run(Scheduled
ThreadPoolExecutor.java:304)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1160)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:635
at java.lang.Thread.run(Thread.java:811)
```

3. Log in to System Manager.
4. On the System Manager web interface, click **Elements** > Avaya Breeze® > **Cluster Administration**.
5. Select the cluster.
6. Click **Certificate Management**.
7. Update or install an Identity Certificate.

Video disabled by default Workspaces agent

Solution

1. Log in to Communication Manager.
2. Set the signaling group to **1**.
3. Set **Direct IP-IP Audio Connections** to `y`.

Troubleshooting for Avaya WebRTC Connect customers

Video calls do not work with the Avaya Aura® Web Gateway Reference Client

Solution

1. On the System Manager web interface, check the Avaya Aura® Web Gateway and Avaya Media Server licenses.
2. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<AMS_EM_FQDN>:8443/emlogin/`
3. Click **System Configuration** > **Server Profile** > **General Settings**.
4. Select the **Firewall NAT Tunneling Media Processor** and **Video Media Processor** check boxes.
5. Click **Save**.

Avaya Aura® Web Gateway auth token error

Solution

1. Log on to the Avaya Aura® Web Gateway with your SSH credentials.
2. Navigate to `/opt/Avaya/CallSignalingAgent/version/mss/8.0.1-4_8.0.26/telportal/webapps`.
3. Rename the token generation file from `service.undeploy` to `generationservice.war`.
4. Rename the `devclient.undeploy` file to `devclient.war`.
5. To restart the Avaya Aura® Web Gateway, run the following command:

   `svc csa restart`

Unable to make a call from iOS

Condition

Your iOS device is unable to recognize the `.pem` file after the file is exported from System Manager. It also displays the following error:

```
Token Request Error. The certificate for this server is invalid.
You might be connecting to a server that is pretending to
be "pusntzd205.apac.avaya.com" which could put your confidential
information at risk.
```

Solution

Change the extension of the `.pem` file to `.crt`.

Note:

The proposed solution is for the iPhone 6s, version 13.4.1.

Application Enablement Services and Call Server Connector service connections fail

Condition

Device, Media and Call Control (DMCC) connection, connecting Application Enablement Services (AES) and Call Server Connector service is not displayed.

Solution

Need to mention the same voice provider id on Call Server Connector attributes and restarting CSC service resolved it

1. Match the Voice Provider ID with Avaya Control Manager (ACM).
2. Add the same Voice Provider ID for Call Server Connector (CSC) attributes.
3. Restart CSC.

Video icon gets disabled for Workspaces agent after answering the video call

Condition

There is no video stream from agent after answering the video call.

Solution

Enable video configurations on Communication Manager, AAWG-AMS and Breeze-AMS as follows.

Task	Description
Configuring media servers for Web Video	Configuring media servers for Web Video on page 94

Table continues…

Task	Description
Configuring an IP codec set for Video	Configuring an IP codec set for Video on page 94
Configuring the signaling group for Web Video	Configuring the signaling group for Web Video on page 92
Configuring customer options	Configuring customer options on page 91
Configuring an IP network region	Configuring an IP network region on page 93

Workspaces agent enters a Not Ready state while answering the calls on Chrome browser

Condition

Workspaces agent is entering in to a Not-Ready state while answering the calls on a Chrome browser.

Chrome browser settings for 86+ versions.

Solution

Update the Chrome browser settings for 86+ versions.

Disable the following parameter in the agent's browser mDNS:

#temporary-unexpire-flags-m85

Issues with ACM

Condition

- Unable to create a user on Avaya Control Manager.

  Synchronization between Avaya Control Manager and Communication Manager does not work.
- Enabling video for the Avaya Control Manager user results in the following error: `Operation unsuccessful.`

Solutions

- Ensure that while creating an Avaya Control Manager user, you did not choose an existing Avaya Control Manager agent.
- For synchronization issues between Avaya Control Manager and Communication Manager, try to synchronize one entity at time.

  Ensure that the entities exist on Communication Manager.
- Ensure that the SIP extension that you assigned to the Avaya Control Manager user is synchronized with Avaya Control Manager.

  You can also run a general Avaya Control Manager synchronization to resolve such issues.

Media not going through Session Border Controller

Solution

Check whether Avaya Aura® Web Gateway has the **Enable port for remote access** attribute enabled for handling the media for external users.

Chapter 14: Log collection procedures

Log collection is the process of collecting log entries from server side and agent side components. Use the following checklist for log collection:

No.	Component	Description	✔
Server Side			
1	Communication Manager	Collect the MST traces.	
2	Session Manager	Collect the SIP traces using *traceSM* utility on Avaya Aura® Session Manager.	
3	Avaya Aura® Media Server	See Collecting Avaya Aura Media Server logs on page 146.	
4	Avaya Aura® Web Gateway	See Collecting Avaya Aura Web Gateway logs on page 147.	
5	Avaya Session Border Controller	See Collecting Avaya Session Border Controller logs on page 147.	
6	Avaya Aura® Device Services	See Collecting Avaya Aura Device Services logs on page 148.	
7	Avaya Breeze®	See Collecting Avaya Avaya Breeze logs on page 148.	
Agent Side			
8	Avaya Workspaces	See Collecting logs from Avaya Workspaces on page 149.	
9	Developer Tool	See Logs from the developer tool on page 149.	
10	Customer Reference Client Logs	See WebRTC Connect Customer Reference Client logs on page 150.	

Collecting Avaya Aura® Media Server logs

Procedure

1. Log on to Avaya Aura® Media Server Element Manager.
2. Navigate to **System Configuration** > **Debug Tracing** > **General Settings**.
3. In the **Debug Logging** field, select `Enabled`.
4. Click **Save**.

5. To collect the logs, navigate to **Tools** > **Log Capture**.
6. Select the **Include trace logs** check box.
7. Click **Download**.

Collecting Avaya Aura® Web Gateway logs

Procedure

1. Log on to Avaya Aura® Web Gateway Element Manager.
2. On the left pane, click **Log Management**.
3. In the **Adjust Service Logging Level** area, in the **Current logging level** field, select `FINEST - All possible messages.`
4. Click **Save**.
5. In the **Adjust Service Logs Retention** area, select the **Use Logs Retention** check box.
6. In the **Collect Logs** area, in the **Number of rotated log files to collect (1-20)**, enter the number of files to include from the log file history.
7. Click **Collect**.
8. Click **Download**.

Collecting Avaya Session Border Controller logs

Before you begin

Log on to Avaya Session Border Controller server command-line interpreter (CLI) and collect the SIP traces using *traceSBC* utility.

Procedure

1. Log on to Avaya Session Border Controller Element Manager Service.
2. Navigate to **Monitoring & Logging** > **Debugging** > **Subsystem Logs**.
3. Select the **Debug** check box.
4. Click **Save**.
5. To collect the logs, navigate to **Monitoring & Logging** > **Log Collection** > **Collect Logs**.
6. Select the **All Logs** check box.
7. In the **From Date & Time** field, enter the date and time from which the logs are be included.

8. In the **To Date & Time** field, enter the data and time upto which the logs are to be collected.
9. Click **Collect Logs**.
10. To download the logs, click the download link displayed by the system after the successful log collection.

Collecting Avaya Aura® Device Services logs

Procedure

1. Log on to Avaya Aura® Device Services Element Manager Service.
2. In the left pane, click **Logs Management** > **Log Level**.
3. In the **Current logging level** field, select `FINEST - All possible messages.`
4. Click **Save**.
5. In the **Collect Logs** area, in the **Number of rotated log files to collect (1-20)**, enter the number of files to include from the log file history.
6. Click **Collect**.
7. Click **Download**.

Collecting Avaya Avaya Breeze® logs

Before you begin

Log on to Avaya Breeze® command-line interpreter (CLI) and execute the following commands:

- **`ce dlogon`** - To log on to CLI.
- **`ce dlogw`** - Create a log *asm.log.xxx*. Reproduce the issue.
- **`ctrl-c`** - To stop the **`ce dlogw`** command.
- **`ce dlogoff`** - After the logs collection process completes, to stop logging, run the **`ce dlogoff`** command.

Procedure

1. Log on to Avaya Aura® System Manager.
2. Navigate to **Elements** > **Avaya Breeze**.
3. In the left pane, click **Configuration** > **Logging**.
4. In the **Cluster** field, select the required cluster.
5. In the **Server** field, select the required server.

6. In the **Service** field, select the service.
7. In the **Log Level** field, select `FINEST`.
8. Click **Set Log Level**.
9. To collect the logs, log in to each node of each cluster and run the following command:

   `ce-report -c1 -sg`

   For example: **`$ ce-report -h`**

```
Usage: ce-report [-d] [-p] [-n] [-c <7>] [-l] [-b] [-s] [-g] [-q]
  -d: include latest dumps
  -p: include performance data
  -n: run at normal priority
  -c: include number of days to collect logs default is 7
  -l: include list of open files - warning this can be very large
  -b: include the breeze database
  -s: include SnapIn service logs
  -g: include data grid logs
  -q: non interactive mode for sdm
```

10. Log into each node of each cluster through **WinSCP**.
11. Copy the logs from `/var/tmp/` to local drive.

Collecting logs from Avaya Workspaces

Procedure

1. Log on to Avaya Workspaces.
2. Click **Settings**.
3. Click the **Logs** tab and select the required session log.

   Note:

   The default option selected is **Full session (Default)**.
4. Click **Download**.

Logs from the developer tool

Procedure

1. Log on to Avaya Workspaces.
2. Press **F12**.

   The Developer page opens.
3. On the Developer tool, click **Applications**.

4. In the left pane, expand **Local Storage**.
5. Select the node under this tree and add a key **_cc.debug** with value = `true`.
6. Click **Refresh** icon to refresh the page.

WebRTC Connect Customer Reference Client logs

About this task

If you are using Avaya provided WebRTC Connect Customer Reference Client, use the following procedure to collect the logs.

Procedure

1. Log on to Elite™ WebRTC Reference Client.
2. From any reference client such as, JavaScript, iOS or Android, for the issue, click the **Hamburger (…)** icon on the top right corner .
3. Click **Send Logs** and enter the email address to which the logs are to be sent to.
4. Click **Send**.

Chapter 15: Troubleshooting

Troubleshooting the Avaya Aura® Web Gateway TestApp issues

Troubleshooting Error 401

Condition

Error 401 unauthorized.

Cause

The port number in the earlier release of Avaya Aura® Web Gateway was 8443, which is no longer valid for the latest release.

Solution

Change the port number to 8445.

Troubleshooting the activation issue

Condition

Unable to activate.

Cause

Session Manager might not be configured to use System Manager certificates.

Solution

Configure Session Manager to use System Manager certificates.

Troubleshooting Avaya WebRTC Connect

Troubleshooting for Avaya WebRTC Connect agents

Failed to activate an agent

Solution

1. In the browser, do the following:
   a. Accept the certificates for the Avaya Aura® Device Services URL:

      `https://<Avaya Aura Device Services_FQDN>/acs/resources`

   b. Accept the certificates for the Avaya Aura® Web Gateway URL:

      `https://<Avaya Aura Web Gateway_FQDN>/csa/resources/tenants/default`

   c. Refresh the page and retry agent activation.
2. To accept the certificates, do the following:
   a. Clear the browser cache and repeat Step 1.
   b. **(Optional)** Restart the browser as a guest user and go to the Avaya Workspaces URL.
3. Go to the following URL for Avaya Aura® Device Services automatic configuration:

   `https://<Avaya Aura Device Services_FQDN>:8443/acs/resources/configurations`

   You can view an output similar to the following:

```
## File Generation Notes
## Avaya Dynamic Configuration Service does not recognize User-Agent -
SET SIPSECURE 0
SET SIPENABLED 1
SET SIPDOMAIN oceana.com
SET SIPUSERNAME 8832018
SET SIPHA1 b459b107705c7277cf936acb3b476d5c
SET ACSPORT 8843
SET ACSSECURE 1
SET ACSENABLED 1
SET ACSSSO 1
SET SIP_CONTROLLER_LIST 10.133.34.202:5061;transport=TLS
SET ACSSRVR 10.133.34.204
SET SIPPROXYSRVR 10.133.34.202
SET SIPPORT 5061
SET LOCKED_PREFERENCES "SIPSECURE,SIPENABLED,SIPDOMAIN,SIPUSERNAME,SIPl
SET OBSCURE_PREFERENCES ""
```

4. **(Optional)** If you do not receive an output with the user configuration details, do the following:
   a. Go to **Start** > **Administrative tools** > **Active Directory** and check if the email field is populated.
   b. **(Optional)** If the email field is empty, specify the user email in the `username@domain` format.

c. Ensure that the user is added to the group that is used for publishing in Avaya Aura® Device Services.

d. On the Avaya Aura® Device Services web interface, click **Server Connections** > **LDAP Configuration**.

e. On the LDAP Configurations page, ensure that the **Role Filter** and **Role Attribute ID** fields are populated.

f. In **User Role**, type the LDAP group name.

For more information about the LDAP group name configuration, see *Administering Avaya Aura® Device Services*.

g. On the Avaya Aura® Device Services web interface, click **Dynamic Configuration** > **Configuration** > **Group**.

h. On the Group page, configure the following parameters:

```
COMM_ADDR_HANDLE_TYPE = Avaya SIP

COMM_ADDR_HANDLE_LENGTH = <Length of your SIP Extensions>
```

i. Publish the LDAP group configuration.

5. Check the connection between Avaya Control Manager and UCAStoreService.
6. Check the CTI-Link from Communication Manager to the Application Enablement Services server.
7. Check whether as common certificate along with the Certificate Authority (CA) certificate is installed on the client machine.
8. Check whether Avaya Aura® Web Gateway and Avaya Aura® Device Services FQDNs are correctly configured in the UnifiedAgentController attributes.

Authentication failures

Solution

1. Check the connection between Avaya Aura® System Manager and LDAP server.
2. Check the LDAP synchronization on the User Management page in System Manager.
3. Check LDAP certificates on all Avaya Breeze® platform nodes.
4. Check authorization certificates update at the cluster level.
5. Ensure that a common certificate is installed on Avaya Breeze® platform nodes, Avaya Aura® Web Gateway, and Avaya Aura® Device Services.
6. Check whether the common certificates are expired.

Avaya Workspaces displays an error in registering the agent

Solution

1. Check the Avaya Aura® Device Services and LDAP connection on Avaya Aura® Device Services.
2. Check the Avaya Aura® Web Gateway and LDAP connection on Avaya Aura® Web Gateway.

3. Check whether a SIP handle is assigned to the System Manager user.
4. Check whether the LDAP users are assigned to the same group configured and published on Avaya Aura® Device Services.
5. Check whether the **Type of 3PCC Enabled** is set as `Avaya` on the Station page of the SIP station assigned to the Avaya Workspaces agent.

Avaya Workspaces displays the Provider not found error

Solution

1. Check the connection between the Call Server Connector (CSC) service and Application Enablement Services server.
2. Check the connection between Avaya Control Manager and UCAStoreService.
3. Check the CTI-Link from Communication Manager to the Application Enablement Services server.
4. Create a new agent in Avaya Control Manager.
5. Restart the Unified Agent Controller (UAC) cluster.
6. Redeploy the UAC cluster.

Cannot change agent states in Avaya Workspaces

Condition

Agent retains the Reconnecting state on Avaya Workspaces.

Solution

1. Close the existing TSAPI sessions on Application Enablement Services (AES).
2. After sessions are recreated, restart AES.
3. Reboot AES.
4. Ensure that the **Date/Time** value is the same on AES, CM, and nodes.
5. Check the CTI-Link from Communication Manager to the AES server, unlink the link, and add it again.
6. Check the connection between the Call Server Connector (CSC) service and AES server.
7. Restart the AES TSAPI and DMCC services.
8. Reboot the cluster.

Authorization error on Workspaces

Condition

Avaya Workspaces displays the following error:

```
Unable to contact the authentication server. Please try again, and if
the problem persists please contact your system administrator.
```

Solution

1. Add the AD certificates again on each node.

2. Restart the cluster.
3. Reinstall Authorization Service.

Unable to contact the authentication server on Workspaces

Solution

1. Ensure that the LDAP password is not reset.
2. On the System Manager web interface, click **Users** > **Directory Synchronization** and check the LDAP connection.
3. To Reinstall the LDAP certificate on the Session Manager and all the nodes, do the following:
    a. On the System Manager web interface, click **Services** > **Inventory** > **Manage Elements**.
    b. On the Manage Elements page, select the check box for one of the nodes of the proposed cluster.
    c. Click **More actions** > **Manage Trusted Certificates**.
    d. On the Manage Trusted Certificates page, click **Add**.
    e. On the Add Trusted Certificate page, do the following:
        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**.

Communication package error on Avaya Workspaces

Solution

1. Restart the Unified Agent Controller (UAC) cluster.
2. **(Optional)** If restarting the cluster does not solve the issue, redeploy the UAC cluster.

Error 404 on Workspaces

Solution

1. Go to **Logs of Authorization**.
2. Ensure that the log file shows the following error:

```
java.lang.IllegalArgumentException: Service AuthorizationService-3.7.0.0.370008
cannot be found on cluster
at
com.avaya.zephyr.platform.dao.AusServiceLevelTLSVersionDAO.getServiceLevelTLSVersi
onForMyCluster(AusServiceLevelTLSVersionDAO.java:228)
at
com.avaya.collaboration.ssl.util.SSLUtilityHelper.getClusterTLSVersion(SSLUtilityH
elper.java:61)
at
com.avaya.collaboration.ssl.util.SSLUtilityImpl.getClusterTLSVersion(SSLUtilityImp
```

```
l.java:405)
at
com.avaya.collaboration.ssl.util.SSLUtilityImpl.createSSLContext(SSLUtilityImpl.ja
va:85)
at
com.avaya.collaboration.ssl.util.SSLUtilityFactoryImpl.createSSLContext(SSLUtility
FactoryImpl.java:25)
at
com.avaya.collaboration.ssl.util.SSLUtilityFactory.createSSLContext(SSLUtilityFact
ory.java:104)
at
com.avaya.zephyr.services.production.AuthorizationService.startup.StartupServlet.i
nitializeHttpClient(StartupServlet.java:169)
at
com.avaya.zephyr.services.production.AuthorizationService.startup.StartupServlet.l
ambda$initializeHttpClient$0(StartupServlet.java:186)
at
com.avaya.zephyr.services.production.AuthorizationService.startup.StartupServlet$
$Lambda$50.0000000022C48410.run(Unknown Source)
at java.util.concurrent.Executors$RunnableAdapter.call(Executors.java:522)
at java.util.concurrent.FutureTask.run(FutureTask.java:277)
at
java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.access$201(Sc
heduledThreadPoolExecutor.java:191)
at
java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.run(Scheduled
ThreadPoolExecutor.java:304)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1160)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:635
at java.lang.Thread.run(Thread.java:811)
```

3. Log in to System Manager.
4. On the System Manager web interface, click **Elements** > Avaya Breeze® > **Cluster Administration**.
5. Select the cluster.
6. Click **Certificate Management**.
7. Update or install an Identity Certificate.

Video disabled by default Workspaces agent

Solution

1. Log in to Communication Manager.
2. Set the signaling group to **1**.
3. Set **Direct IP-IP Audio Connections** to `y`.

Troubleshooting for Avaya WebRTC Connect customers

Video calls do not work with the Avaya Aura® Web Gateway Reference Client

Solution

1. On the System Manager web interface, check the Avaya Aura® Web Gateway and Avaya Media Server licenses.

2. In your web browser, enter the following URL to log on to Avaya Aura® Media Server Element Manager:

   `https://<AMS_EM_FQDN>:8443/emlogin/`

3. Click **System Configuration** > **Server Profile** > **General Settings**.
4. Select the **Firewall NAT Tunneling Media Processor** and **Video Media Processor** check boxes.
5. Click **Save**.

Avaya Aura® Web Gateway auth token error

Solution

1. Log on to the Avaya Aura® Web Gateway with your SSH credentials.
2. Navigate to `/opt/Avaya/CallSignalingAgent/version/mss/8.0.1-4_8.0.26/telportal/webapps`.
3. Rename the token generation file from `service.undeploy` to `generationservice.war`.
4. Rename the `devclient.undeploy` file to `devclient.war`.
5. To restart the Avaya Aura® Web Gateway, run the following command:

   `svc csa restart`

Unable to make a call from iOS

Condition

Your iOS device is unable to recognize the `.pem` file after the file is exported from System Manager. It also displays the following error:

```
Token Request Error. The certificate for this server is invalid.
You might be connecting to a server that is pretending to
be "pusntzd205.apac.avaya.com" which could put your confidential
information at risk.
```

Solution

Change the extension of the `.pem` file to `.crt`.

Note:

The proposed solution is for the iPhone 6s, version 13.4.1.

Application Enablement Services and Call Server Connector service connections fail

Condition

Device, Media and Call Control (DMCC) connection, connecting Application Enablement Services (AES) and Call Server Connector service is not displayed.

Solution

Need to mention the same voice provider id on Call Server Connector attributes and restarting CSC service resolved it

1. Match the Voice Provider ID with Avaya Control Manager (ACM).
2. Add the same Voice Provider ID for Call Server Connector (CSC) attributes.
3. Restart CSC.

Video icon gets disabled for Workspaces agent after answering the video call

Condition

There is no video stream from agent after answering the video call.

Solution

Enable video configurations on Communication Manager, AAWG-AMS and Breeze-AMS as follows.

Task	Description
Configuring media servers for Web Video	Configuring media servers for Web Video on page 94
Configuring an IP codec set for Video	Configuring an IP codec set for Video on page 94
Configuring the signaling group for Web Video	Configuring the signaling group for Web Video on page 92
Configuring customer options	Configuring customer options on page 91
Configuring an IP network region	Configuring an IP network region on page 93

Workspaces agent enters a Not Ready state while answering the calls on Chrome browser

Condition

Workspaces agent is entering in to a Not-Ready state while answering the calls on a Chrome browser.

Chrome browser settings for 86+ versions.

Solution

Update the Chrome browser settings for 86+ versions.

Disable the following parameter in the agent's browser mDNS:

#temporary-unexpire-flags-m85

Issues with ACM

Condition

- Unable to create a user on Avaya Control Manager.

Synchronization between Avaya Control Manager and Communication Manager does not work.

- Enabling video for the Avaya Control Manager user results in the following error: `Operation unsuccessful`.

Solutions

- Ensure that while creating an Avaya Control Manager user, you did not choose an existing Avaya Control Manager agent.
- For synchronization issues between Avaya Control Manager and Communication Manager, try to synchronize one entity at time.

  Ensure that the entities exist on Communication Manager.
- Ensure that the SIP extension that you assigned to the Avaya Control Manager user is synchronized with Avaya Control Manager.

  You can also run a general Avaya Control Manager synchronization to resolve such issues.

Media not going through Session Border Controller

Solution

Check whether Avaya Aura® Web Gateway has the **Enable port for remote access** attribute enabled for handling the media for external users.

Log collection procedures

Log collection is the process of collecting log entries from server side and agent side components. Use the following checklist for log collection:

No.	Component	Description	✔
Server Side			
1	Communication Manager	Collect the MST traces.	
2	Session Manager	Collect the SIP traces using *traceSM* utility on Avaya Aura® Session Manager.	
3	Avaya Aura® Media Server	See Collecting Avaya Aura Media Server logs on page 146.	
4	Avaya Aura® Web Gateway	See Collecting Avaya Aura Web Gateway logs on page 147.	
5	Avaya Session Border Controller	See Collecting Avaya Session Border Controller logs on page 147.	
6	Avaya Aura® Device Services	See Collecting Avaya Aura Device Services logs on page 148.	

Table continues…

No.	Component	Description	✔
7	Avaya Breeze®	See Collecting Avaya Avaya Breeze logs on page 148.	
Agent Side			
8	Avaya Workspaces	See Collecting logs from Avaya Workspaces on page 149.	
9	Developer Tool	See Logs from the developer tool on page 149.	
10	Customer Reference Client Logs	See WebRTC Connect Customer Reference Client logs on page 150.	

Collecting Avaya Aura® Media Server logs

Procedure

1. Log on to Avaya Aura® Media Server Element Manager.
2. Navigate to **System Configuration** > **Debug Tracing** > **General Settings**.
3. In the **Debug Logging** field, select `Enabled`.
4. Click **Save**.
5. To collect the logs, navigate to **Tools** > **Log Capture**.
6. Select the **Include trace logs** check box.
7. Click **Download**.

Collecting Avaya Aura® Web Gateway logs

Procedure

1. Log on to Avaya Aura® Web Gateway Element Manager.
2. On the left pane, click **Log Management**.
3. In the **Adjust Service Logging Level** area, in the **Current logging level** field, select `FINEST - All possible messages`.
4. Click **Save**.
5. In the **Adjust Service Logs Retention** area, select the **Use Logs Retention** check box.
6. In the **Collect Logs** area, in the **Number of rotated log files to collect (1-20)**, enter the number of files to include from the log file history.
7. Click **Collect**.
8. Click **Download**.

Collecting Avaya Session Border Controller logs

Before you begin

Log on to Avaya Session Border Controller server command-line interpreter (CLI) and collect the SIP traces using *traceSBC* utility.

Procedure

1. Log on to Avaya Session Border Controller Element Manager Service.
2. Navigate to **Monitoring & Logging** > **Debugging** > **Subsystem Logs**.
3. Select the **Debug** check box.
4. Click **Save**.
5. To collect the logs, navigate to **Monitoring & Logging** > **Log Collection** > **Collect Logs**.
6. Select the **All Logs** check box.
7. In the **From Date & Time** field, enter the date and time from which the logs are be included.
8. In the **To Date & Time** field, enter the data and time upto which the logs are to be collected.
9. Click **Collect Logs**.
10. To download the logs, click the download link displayed by the system after the successful log collection.

Collecting Avaya Aura® Device Services logs

Procedure

1. Log on to Avaya Aura® Device Services Element Manager Service.
2. In the left pane, click **Logs Management** > **Log Level**.
3. In the **Current logging level** field, select `FINEST - All possible messages`.
4. Click **Save**.
5. In the **Collect Logs** area, in the **Number of rotated log files to collect (1-20)**, enter the number of files to include from the log file history.
6. Click **Collect**.
7. Click **Download**.

Collecting Avaya Avaya Breeze® logs

Before you begin

Log on to Avaya Breeze® command-line interpreter (CLI) and execute the following commands:

- **`ce dlogon`** - To log on to CLI.

- **`ce dlogw`** - Create a log *asm.log.xxx*. Reproduce the issue.
- **`ctrl-c`** - To stop the **`ce dlogw`** command.
- **`ce dlogoff`** - After the logs collection process completes, to stop logging, run the **`ce dlogoff`** command.

Procedure

1. Log on to Avaya Aura® System Manager.
2. Navigate to **Elements** > **Avaya Breeze**.
3. In the left pane, click **Configuration** > **Logging**.
4. In the **Cluster** field, select the required cluster.
5. In the **Server** field, select the required server.
6. In the **Service** field, select the service.
7. In the **Log Level** field, select `FINEST`.
8. Click **Set Log Level**.
9. To collect the logs, log in to each node of each cluster and run the following command:

   `ce-report -c1 -sg`

   For example: **`$ ce-report -h`**

```
Usage: ce-report [-d] [-p] [-n] [-c <7>] [-l] [-b] [-s] [-g] [-q]
  -d: include latest dumps
  -p: include performance data
  -n: run at normal priority
  -c: include number of days to collect logs default is 7
  -l: include list of open files - warning this can be very large
  -b: include the breeze database
  -s: include SnapIn service logs
  -g: include data grid logs
  -q: non interactive mode for sdm
```

10. Log into each node of each cluster through **WinSCP**.
11. Copy the logs from `/var/tmp/` to local drive.

Collecting logs from Avaya Workspaces

Procedure

1. Log on to Avaya Workspaces.
2. Click **Settings**.
3. Click the **Logs** tab and select the required session log.

   Note:

   The default option selected is **Full session (Default)**.
4. Click **Download**.

Logs from the developer tool

Procedure

1. Log on to Avaya Workspaces.
2. Press **F12**.

   The Developer page opens.
3. On the Developer tool, click **Applications**.
4. In the left pane, expand **Local Storage**.
5. Select the node under this tree and add a key **_cc.debug** with value = `true`.
6. Click **Refresh** icon to refresh the page.

WebRTC Connect Customer Reference Client logs

About this task

If you are using Avaya provided WebRTC Connect Customer Reference Client, use the following procedure to collect the logs.

Procedure

1. Log on to Elite™ WebRTC Reference Client.
2. From any reference client such as, JavaScript, iOS or Android, for the issue, click the **Hamburger (…)** icon on the top right corner .
3. Click **Send Logs** and enter the email address to which the logs are to be sent to.
4. Click **Send**.

Chapter 16: Related resources

Documentation

Title	Use this document to:	Audience
Avaya Workspaces for Call Center Elite Solution Description	Learn about the product's key features, capacities, and footprint.	Solution Architects, Sales Engineers, Implementation Engineers
Deploying Avaya Workspaces for Call Center Elite	Deploy and administer Avaya Workspaces for Call Center Elite.	Administrators
Using Avaya Workspaces for Call Center Elite	Use the Avaya Workspaces for Call Center Elite browser-based application.	Contact Center Agents
Avaya Workspaces for Call Center Elite Disaster Recovery	Learn about Avaya Workspaces for Call Center Elite Disaster Recovery, and how to configure Disaster Recovery for your solution.	Solution Architects, Sales Engineers, Implementation Engineers
Planning for Deploying Avaya Aura® applications	Learn about planning for deploying Avaya Aura® applications.	Solution Architects, Sales Engineers, Implementation Engineers
Deploying Avaya Aura® Device Services	Planning, installation, and configuring Avaya Aura® Device Services.	Implementation Engineers
Deploying Avaya Breeze® platform	Learn about installation, configuration, initial administration, and basic maintenance checklist and procedures for Avaya Breeze® platform.	Solution Architects, Implementation Engineers
Deploying the Avaya Aura® Web Gateway	Learn about planning, installation, and configuration of the Avaya Aura® Web Gateway.	Solution Architects, Implementation Engineers
Deploying Avaya Session Border Controller	Install and configure Avaya Session Border Controller (Avaya SBCE) in an enterprise having Session Initiation Protocol (SIP) trunks.	Solution Architects, Implementation Engineers
Using Avaya Workplace Client for Android, iOS, Mac, and Windows	Learn about using Avaya Workplace Client for Android, iOS, Mac, and Windows.	Solution Architects, Implementation Engineers

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click to display the search results.

Viewing Avaya Mentor videos

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

About this task

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

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

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

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.

- Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

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

Related links

Using the Avaya InSite Knowledge Base on page 166

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log in to the Avaya support website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Related links

Support on page 166

Index

M

N

P

R

S

T

U

V

W