# Deploying the Avaya Aura® Web Gateway

Release 3.9
Issue 1
March 2021

**Notice**

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

**Documentation disclaimer**

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

**Link disclaimer**

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

**Warranty**

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

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

**Hosted Service**

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

**Licenses**

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

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

**License types**

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

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

Named User License (NU). End User may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as

only authorized Named Users access and use the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”) as indicated in the order, Documentation, or as authorized by Avaya in writing.

**Heritage Nortel Software**

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

**Copyright**

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

**Virtualization**

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

**Third Party Components**

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

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

**Service Provider**

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

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

**Compliance with Laws**

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

**Preventing Toll Fraud**

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

**Avaya Toll Fraud intervention**

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

**Security Vulnerabilities**

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

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

**Downloading Documentation**

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

**Contact Avaya Support**

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

**Trademarks**

# Contents

# Chapter 1: Introduction

## Purpose

This document provides checklists and procedures for planning, installation, and configuration of the Avaya Aura® Web Gateway. It is intended for customer installers and administrators.

**Note:**

This document does not describe SDK developer applications.

After you deploy Avaya Aura® Web Gateway, see *Administering the Avaya Aura® Web Gateway* for administration and maintenance information. You can also find information about managing Integrated Windows Authentication (IWA) and push notification services in *Administering the Avaya Aura® Web Gateway*.

## Change history

This section describes the major changes made in this document:

| Issue | Date | Summary of changes |
|---|---|---|
| Release 3.9, Issue 1 | March 2021 | • Updated the list of supported VMware versions in VMware software requirements on page 30.<br>• Indicated that virtual machine resource requirements also apply to software-only deployments in Resource profile specifications for Avaya Aura Web Gateway on VMware on page 30.<br>• Added Characters supported for Avaya Aura Web Gateway passwords on page 48.<br>• Added information about software-only deployment options to Deployment process checklist on page 49.<br>• Updated the title of Converting the imported OVA to AMI on page 61.<br>• Updated steps in Creating CloudFormation templates on page 62. |

| Issue | Date | Summary of changes |
|---|---|---|
| | | • Added procedures for installing Avaya Aura® Web Gateway as a software-only application under Software-only deployments on page 73.<br>• Indicated that Cassandra internode encryption must be enabled if FIPS is enabled when installing Avaya Aura® Web Gateway in Installing the Avaya Aura Web Gateway on page 98 and Installing additional nodes to create a cluster on page 104.<br>• Indicated that the Cassandra default password must be changed after Avaya Aura® Web Gateway installation in Installing the Avaya Aura Web Gateway on page 98 and Installing additional nodes to create a cluster on page 104.<br>• Added Unexpected characters in the /etc/hosts file on a localhost line on page 101.<br>• Added Changing the Cassandra user name and password on page 130.<br>• Added Changing the default password for automatic backups on page 131.<br>• Indicated that enabling TURN on the client side is the preferred option in Configuring Avaya Aura Media Server settings on page 141.<br>• Indicated that the web administration portal must be used to manage System Manager certificates in Certificate setup on page 176 and Certificate configuration using the configuration utility on page 188. |

# Chapter 2: Avaya Aura® Web Gateway overview

The Avaya Aura® Web Gateway server acts as a gateway to Avaya Aura® clients and applications utilizing WebRTC signaling and media. Avaya Aura® Web Gateway also provides the push notification service, enabling clients to receive incoming call alerts and other notifications from the Apple Push Notification service (APNs).

You can deploy the Avaya Aura® Web Gateway through Amazon Web Services (AWS), VMware, or Avaya Virtualization Platform.

You can deploy the Avaya Aura® Web Gateway in the following environments:

- Avaya Aura® (Team Engagement)
- Avaya Aura® and Conferencing (Team Engagement and Conferencing)

To access conferencing tools, such as Avaya Meetings Server, your deployment must include Conferencing.

**Note:**

An Over-The-Top (OTT), or Conferencing-only, deployment option is available, but it is not described in this document. The Conferencing-only option follows a different deployment process. For more information, see *Deploying Avaya Meetings Server*.

## New in this release

The following is a summary of new functionality that has been added to the Avaya Aura® Web Gateway in Release 3.9:

### Software-only installation

Avaya Aura® Web Gateway Release 3.9 supports software-only installation. In software-only deployments, you must provide and configure the operating system for use with the Avaya Aura® Web Gateway application. Avaya Aura® Web Gateway supports VMware and AWS virtual environments for software-only installation.

### Red Hat Enterprise Linux 7.6 support

Avaya Aura® Web Gateway now uses Red Hat Enterprise Linux 7.6.

### Performance metrics dashboard

You can now review various performance metrics and system health indicators, such as CPU or memory usage, on the Avaya Aura® Web Gateway web administration portal.

### Automatic backup

Avaya Aura® Web Gateway creates backups of configuration files and user data automatically on a weekly basis. You can modify the default automatic backup settings from the web administration portal.

### Scheduled log collection

You can now enable a specific logging level on a temporary basis for a specified time period. After the specified time period expires, Avaya Aura® Device Services switches back to the original log level.

### Security enhancements

To ensure the secure processing of user data and reduce security vulnerabilities, Avaya Aura® Web Gateway now supports the following features:

- The single-user mode of the RHEL operating system is now password-protected.
- Avaya Aura® Web Gateway now enforces default password policies for all human-user accounts.

### IWA multidomain support

Avaya Aura® Web Gateway now supports IWA for multiple domains. You can now configure multiple active directories to use IWA capabilities.

# Solution architecture

This section provides a graphical representation of the Avaya Aura® Web Gateway deployment architecture.

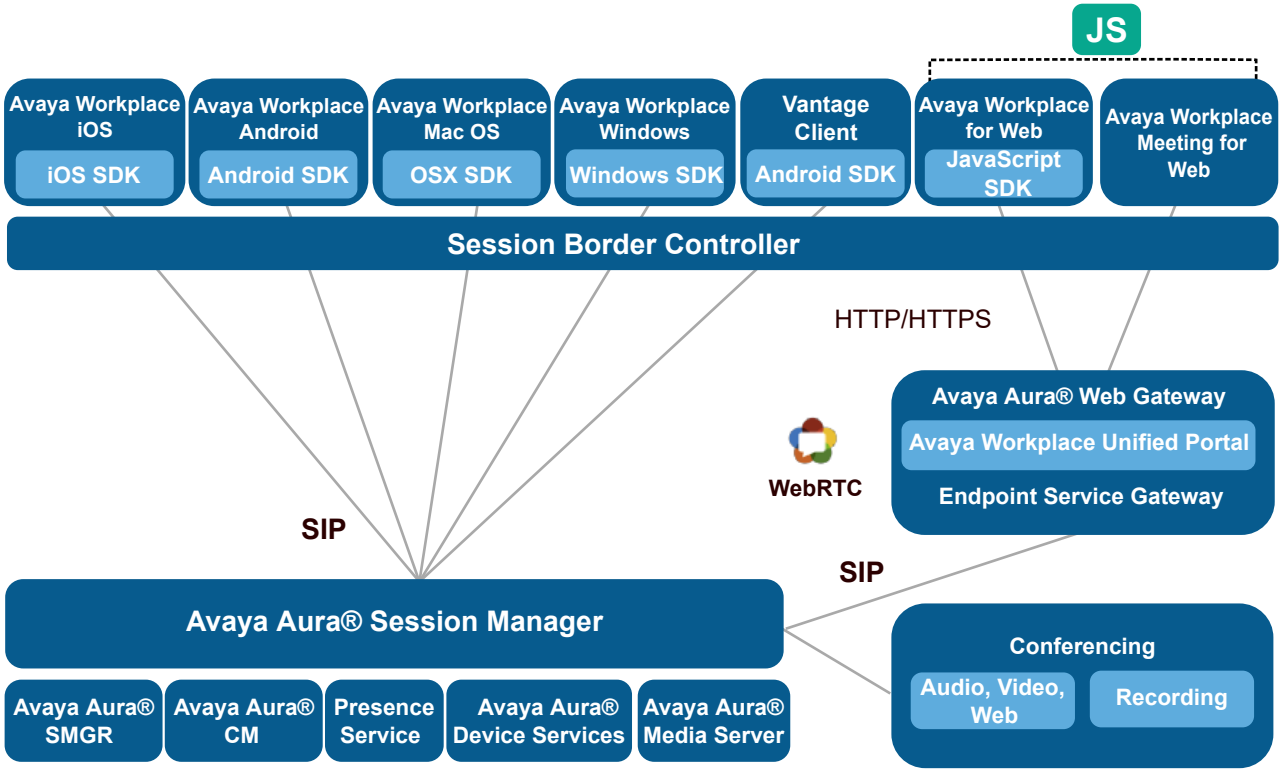
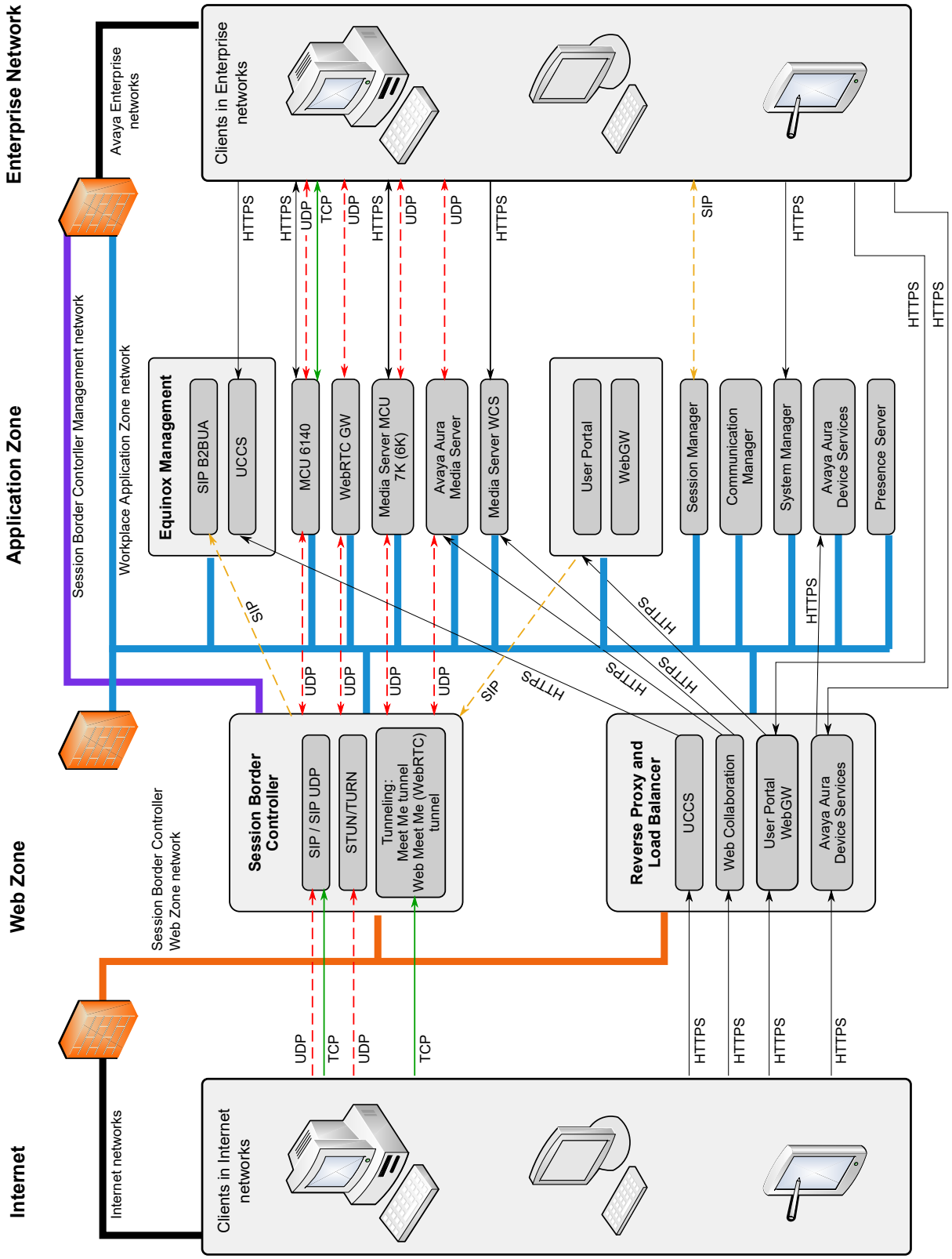



**Figure 1: Avaya Workplace Client and Conferencing deployment topology**

# Topology diagram

This section provides a graphical representation of the Team Engagement + Conferencing deployment model topology.


Enterprise Network
Application Zone
Web Zone
Internet
Clients in Enterprise networks
Avaya Enterprise networks
Session Border Contoller Management network
Workplace Application Zone network
Equinox Management
SIP B2BUA
UCCS
MCU 6140
WebRTC GW
Media Server MCU 7K (6K)
Avaya Aura Media Server
Media Server WCS
User Portal
WebGW
Session Manager
Communication Manager
System Manager
Avaya Aura Device Services
Presence Server
Session Border Controller
SIP / SIP UDP
STUN/TURN
Tunneling: Meet Me tunnel Web Meet Me (WebRTC) tunnel
Reverse Proxy and Load Balancer
UCCS
Web Collaboration
User Portal WebGW
Avaya Aura Device Services
Session Border Controller Web Zone network
Internet networks
Clients in Internet networks
HTTPS
UDP
TCP
SIP

For detailed information about ports, go to https://support.avaya.com/security, scroll down, and click **Avaya Product Port Matrix Documents**. Navigate to the required solution component section and then click on the appropriate Port Matrix document for the release to open it.

# Geographical distribution overview

In a geographically distributed system, resources are deployed in multiple data centers to reduce media delays. For this purpose, the following components are deployed in each data center:

- Avaya Aura® Media Server
- Avaya Aura® Session Border Controller
- Avaya Aura® Web Gateway
- Web Collaboration Server
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Device Services

In a geographically distributed system, you must also install the following two components:

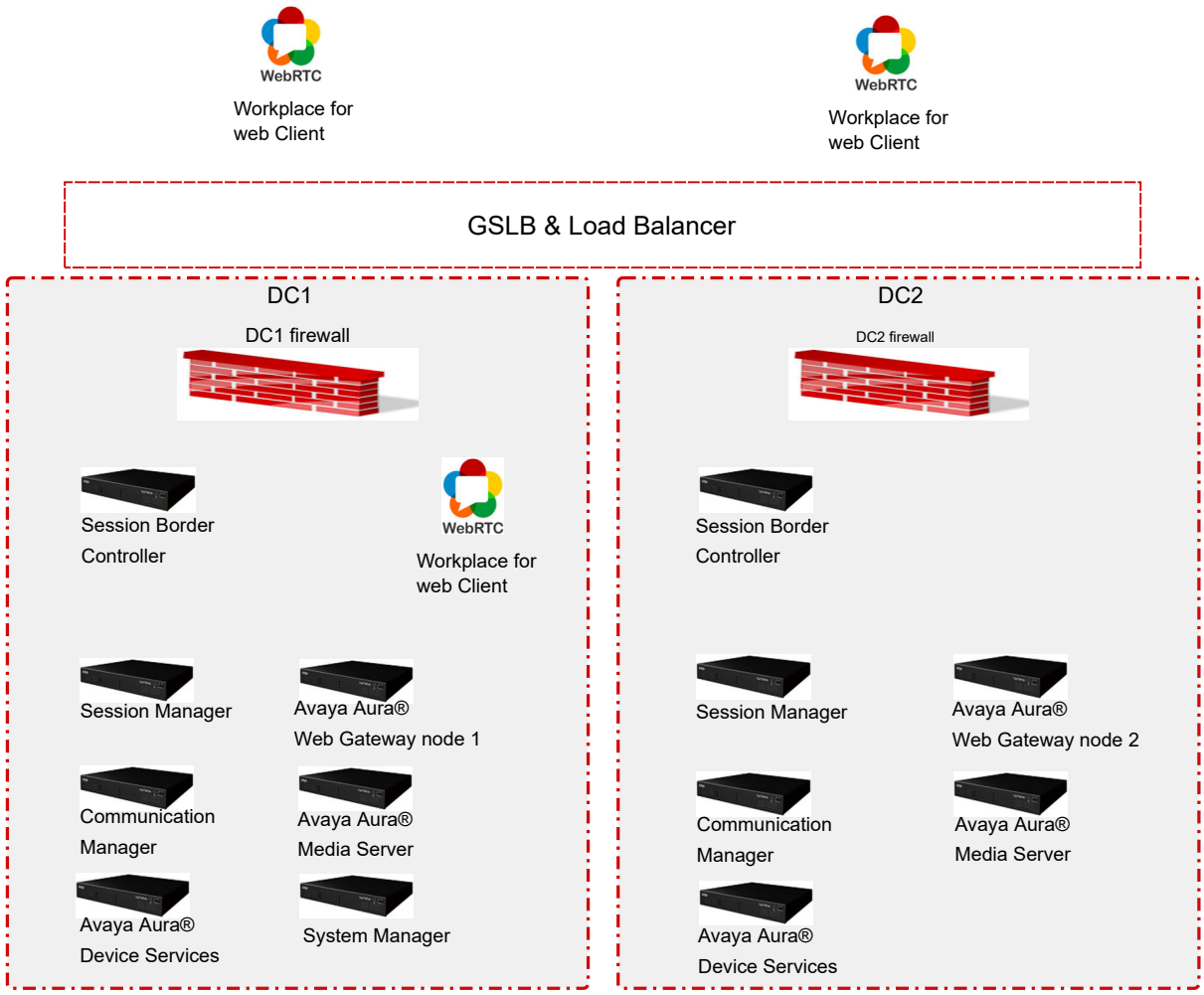
- Global Server Load Balancing (GSLB), which provides different routes and addresses based on the location of the client.
- Load balancer, which balances traffic between two or more Avaya Aura® Web Gateway nodes, which may be located in the same data center or in different data centers.

Avaya Aura® Session Manager and Avaya Aura® Communication Manager are important for call routing. To optimize media delays for point-to-point calls, deploy these components in a distributed manner across your data centers. The way in which these components are geographically distributed is outside the scope of this document. For more information about configuring Session Manager and Communication Manager, see *Administering Avaya Aura® Session Manager* and *Administering Avaya Aura® Communication Manager*.

For more information about configuring a geographically distributed system, see the list of tasks for multiple data centers in Configuration worksheet on page 23.

## General geographical distribution topology

In this topology example, there are two data centers with one Avaya Aura® Web Gateway in each data center. For simplicity, System Manager is deployed in Data Center 1 (DC1), while Session Manager, Communication Manager, and Avaya Aura® Device Services are deployed in all data centers.



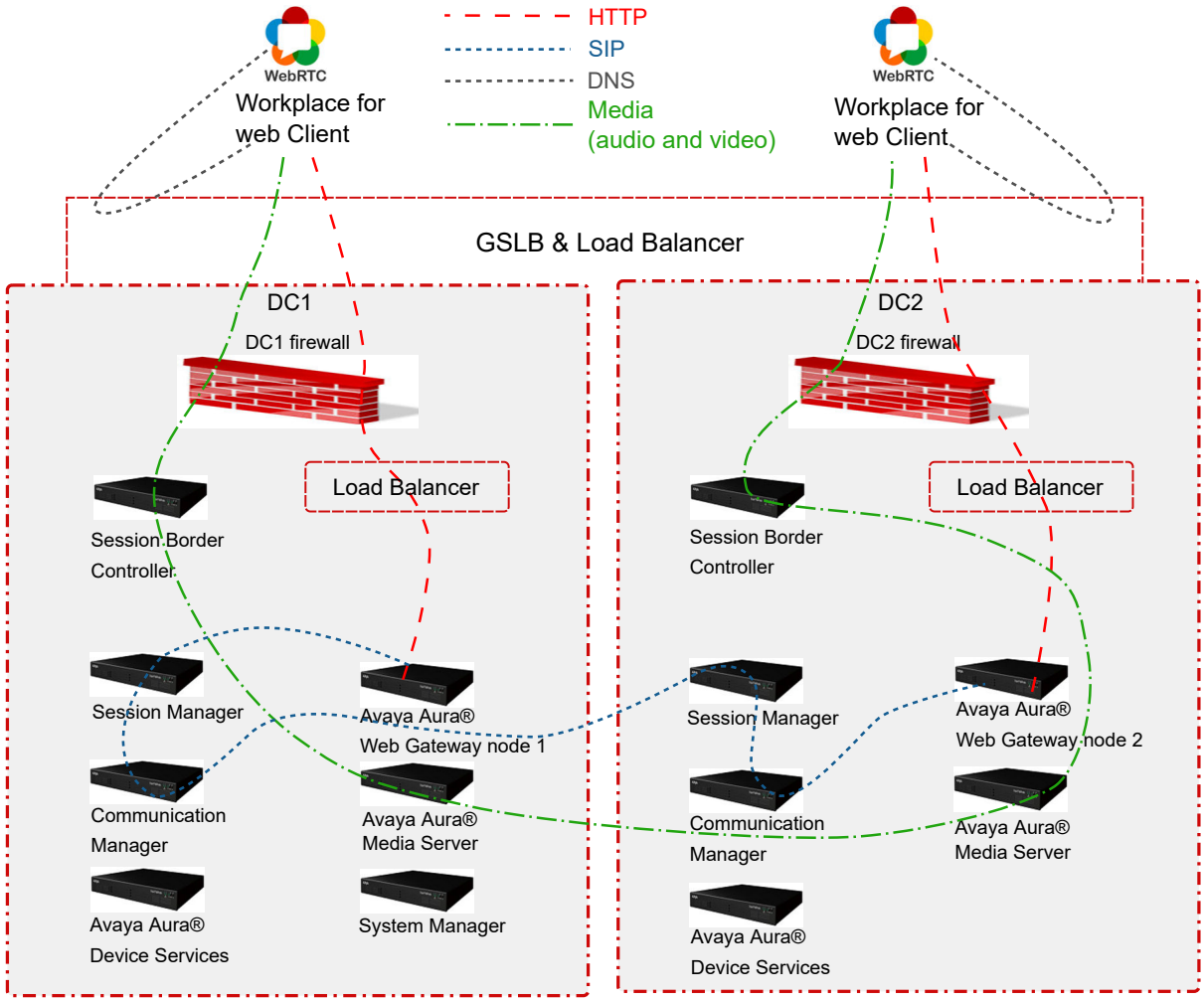

## Signaling and media path topology when clients are located in or near different data centers

In the following topology example, there are two data centers with one Avaya Aura® Web Gateway in each data center. Clients are located in different data centers outside of the firewall and registered on the Avaya Aura® Web Gateway to receive calls. When one client makes a call to the other, the call follows the following flow:

1. Both clients log in to the corresponding Avaya Aura® Web Gateway and activate the call service.
    a. A client in data center 1 (DC1) gets the address of the DC1 load balancer and communicates with the Avaya Aura® Web Gateway deployed on that data center. The Avaya Aura® Web Gateway registers the client to the corresponding Session Manager deployed on DC1.

b. A client in data center 2 (DC2) gets the address of the DC2 load balancer and communicates with the Avaya Aura® Web Gateway deployed on that data center. The Avaya Aura® Web Gateway registers the client to the corresponding Session Manager deployed on DC2.

2. The DC1 Avaya Aura® Web Gateway initiates the call. To route the media, the Avaya Aura® Web Gateway uses the Session Border Controller and Avaya Aura® Media Server deployed on DC1.
3. The Avaya Aura® Web Gateway sends the SIP call to Session Manager deployed on DC1.
4. Session Manager deployed on DC1 forwards the call to Session Manager deployed on DC2.
5. Session Manager deployed on DC2 forwards the SIP invite to the Avaya Aura® Web Gateway from DC2, where the second client is logged in.
6. The Avaya Aura® Web Gateway from DC2 uses the Session Border Controller and Avaya Aura® Media Server deployed on DC2 to pass the media through the firewall to the second client.



## Signalling and media path topology when both clients are located in or near the same data center

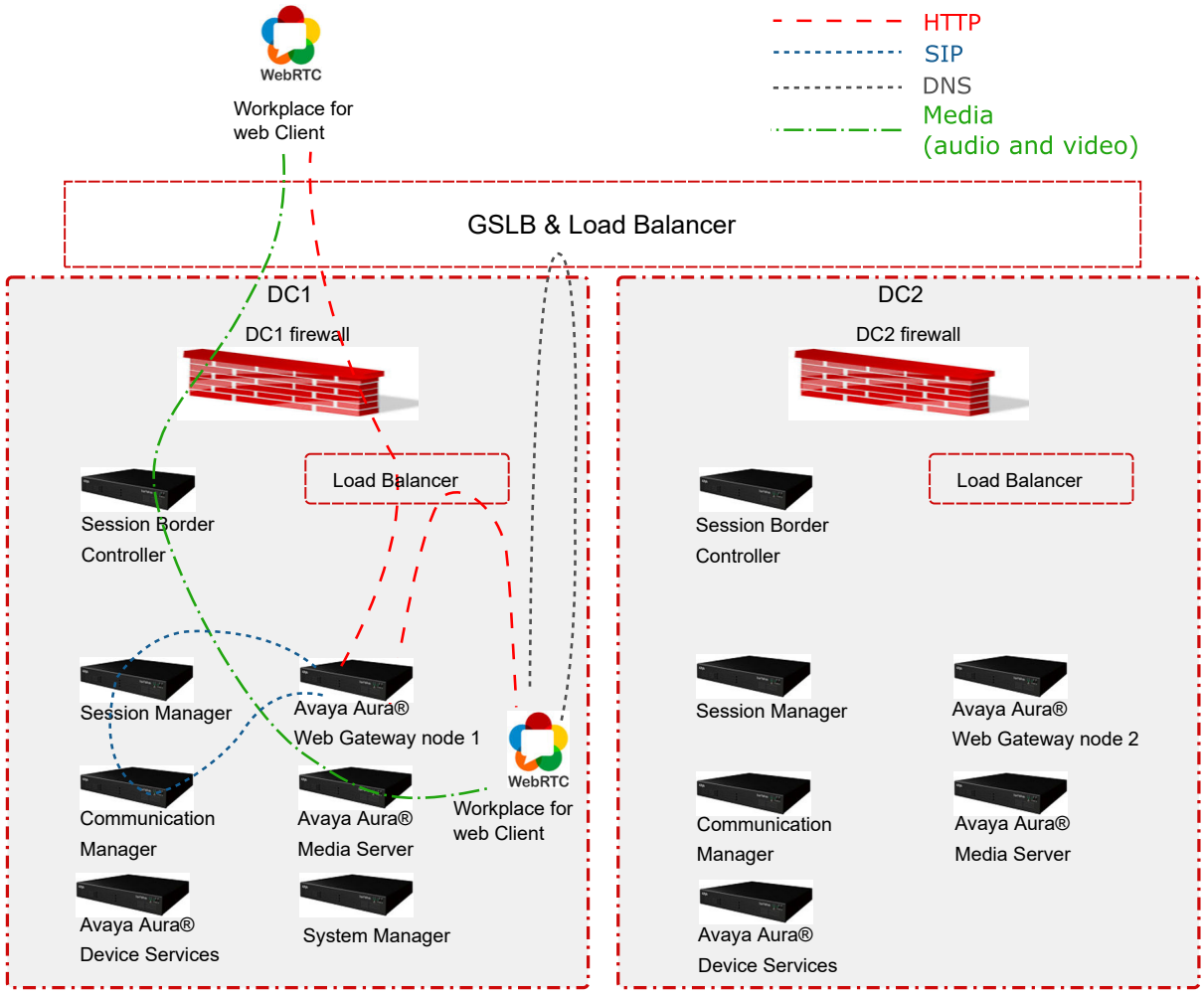
In the following topology example, there are two data centers with one Avaya Aura® Web Gateway in each data center. Two clients are located in or near the same data center (DC1):

- The first client is located outside the firewall.
- The second client is located inside the enterprise network.

Both clients are registered on the Avaya Aura® Web Gateway to receive calls. When one client makes a call to the other, the call follows the following flow:

1. Both clients log in to the Avaya Aura® Web Gateway and activate the call service.

   Both clients resolve the FQDN to the address of the load balancer deployed on DC1 and communicate with the Avaya Aura® Web Gateway deployed on DC1.
2. The external client initiates the call.
3. The Avaya Aura® Web Gateway sends the SIP call to Session Manager deployed on DC1.
4. Session Manager deployed on DC1 forwards the call to the same Avaya Aura® Web Gateway deployed on DC1, where the internal client is logged in.
5. The Avaya Aura® Web Gateway deployed on DC1 uses the Session Border Controller and Avaya Aura® Media Server deployed on DC1 to pass the media through to the internal client.




# Push notifications

The push notification mechanism enables clients to receive incoming call alerts and other notifications from the Apple Push Notification service (APNs). The push notification service sends notifications automatically. Therefore, an application can receive notifications even when it is suspended or in Sleep mode.

The Avaya Aura® Web Gateway can send push notifications about the following telephony-related events:

- Incoming calls.
- Incoming calls on an Avaya Aura® Communication Manager bridged line appearance.
- Incoming calls on an Avaya Aura® Communication Manager enhanced pickup group.
- Incoming calls on an Avaya Aura® Communication Manager team button.

- Voicemail status updates.

For messaging push notifications, use Avaya Multimedia Messaging or Avaya Aura® Presence Services Release 8.0.2 or later.

For more information about configuring and using the push notifications service, see “Avaya push notification management” in *Administering the Avaya Aura® Web Gateway*.

# Data encryption

As of Release 3.8, you can enable or disable data encryption when deploying the Avaya Aura® Web Gateway OVA. When data encryption is enabled, all operational data and log files are encrypted.

You can only enable data encryption on Avaya Aura® Web Gateway if are using Appliance Virtualization Platform or a VMware Virtualized Environment. For Amazon Web Services (AWS) deployments, you must enable data encryption on AWS itself. For more information, see How to Protect Data at Rest with Amazon EC2 Instance Store Encryption.

Once data encryption is enabled, you cannot disable it using the configuration utility or the Avaya Aura® Web Gateway administration portal. To disable data encryption, you must redeploy the Avaya Aura® Web Gateway OVA.

If you enabled data encryption and selected the **Require Encryption Pass-Phrase at Boot-Time** option, then you will need to enter the data encryption passphrase after every Avaya Aura® Web Gateway reboot. If you do not select this option, Avaya Aura® Web Gateway enables the local key store to store encryption keys, so you do not need to enter the passphrase manually. However, this is a less secure solution. Alternatively, you can set up a remote key sever to store encryption keys on that server.

## Encryption of Avaya Aura® Web Gateway partitions

When you enable data encryption for Avaya Aura® Web Gateway, the following partitions are encrypted:

- sdb: `/var/log/Avaya`
- sdc: `/media/data`
- sdd: `/media/cassandra`

The sda boot disk is always unencrypted.

## Data encryption management

After deploying the Avaya Aura® Web Gateway OVA with data encryption enabled, you can manage data encryption settings using system layer commands. For information about managing data encryption settings, see the “Security options” chapter in *Administering the Avaya Aura® Web Gateway*.

# Interoperability

## Product compatibility

Avaya Aura® Web Gateway interacts with the following components. For information about interoperability and supported product versions, see https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml.

| Component | Description |
|---|---|
| Avaya Aura® infrastructure | The following Avaya Aura® components must be installed and configured to use TLS:<br>• Avaya Aura® Device Services: Provides centralized contact management services using REST-based APIs.<br>• Avaya Aura® Media Server: Supports standard media processing features.<br>**Important:**<br>Avaya Aura® Web Gateway does not support Media Server High Availability cluster configuration when using WebRTC.<br>• System Manager: Manages Avaya Aura® components, certificates, licenses, and checks log and alarm capabilities.<br>• Session Manager: Enables applications to perform registration and telephony functions, such as call escalation. |
| Avaya Multimedia Messaging | A server that provides messaging services. |
| Conferencing | This describes the deployment for Avaya Aura® Web Gateway, but not Conferencing itself.<br>The Avaya Meetings Server solution provides conferencing and collaboration functionality.<br>Avaya Meetings Server is not available with the Avaya Aura® Web Gateway Avaya Workplace Client only deployment option. |
| Avaya SBCE | A component that provides a common element to enable secure access to the Avaya infrastructure from untrusted networks, such as the internet. In addition to SIP firewall services, this component provides the Reverse Proxy services required for HTTP signaling, media traversal, and access to other data services. |

## Web browser requirements

The Avaya Aura® Web Gateway administration portal supports the following web browsers:

- Internet Explorer 9, 10, or 11.
- Microsoft Edge 42 and later.
- The latest version of Mozilla Firefox or the version before it.
- Google Chrome 53 and later.

For information about supported browser versions for AWS deployments, see https://aws.amazon.com/console/faqs/#browser_support.

# Chapter 3: Deployment process

The following table shows the high-level tasks for deploying the Avaya Aura® Web Gateway

| High-level tasks | Notes |
|---|---|
| Perform planning and site preparation tasks. | See Planning checklist on page 26.<br>As part of the site preparation, you must set up the required infrastructure components in your network. Avaya Aura® is required in Team Engagement deployments. Your deployment can also include Conferencing. |
| Complete initial setup and installation. | You must deploy the OVA for the VMware or AWS environment before you can install the Avaya Aura® Web Gateway software.<br>See Deployment process checklist on page 49. |
| Perform configuration. | Perform the appropriate configuration tasks for each deployment option. For more information, see Configuration worksheet on page 23. |

## Configuration worksheet

Use this checklist to determine the configuration requirements for each deployment type. The deployment types are:

- Single FQDN, single data center.
- Multiple FQDNs, single data center.
- Multiple data centers, which is also known as geographical distribution.

The deployment option with multiple data centers requires multiple FQDNs. With this deployment, you require at least one FQDN for each service.

| Task | Single FQDN, single data center | Multiple FQDNs, single data center | Multiple data centers |
|---|---|---|---|
| Configure a global FQDNs. See Global FQDN configuration on page 133 | ✔ | — | ✔ |
| Configure Avaya Aura® Web Gateway certificates.<br>**Tip:**<br>When possible, perform certificate configuration in the web administration portal as described in *Administering the Avaya Aura® Web Gateway*. If the web administration portal is not available, see Certificate configuration using the configuration utility on page 188. | ✔<br>For this deployment, use System Manager certificates if possible. | ✔<br>For this deployment, generate a Certificate Signing Request (CSR) and get it signed by a public CA. | ✔<br>For this deployment, use System Manager certificates if possible. |
| Configure System Manager. See Adding the Avaya Aura Web Gateway to System Manager on page 136. | ✔ | ✔ | ✔ |
| Configure Avaya Aura® Media Server. See Configuring Avaya Aura Media Server settings on page 141. | ✔ | ✔ | ✔ |
| Configure Avaya Aura® Device Services. See Configuring the Avaya Aura Web Gateway on Avaya Aura Device Services on page 143. | ✔ | ✔ | ✔ |

*Table continues…*

| Task | Single FQDN, single data center | Multiple FQDNs, single data center | Multiple data centers |
|---|---|---|---|
| If your deployment includes Conferencing, configure Avaya Meetings Server. See Configuring the Avaya Aura Web Gateway on Avaya Meetings Server on page 144. | ✔ | ✔ | ✔ |
| Configure the reverse proxy on Avaya Session Border Controller for Enterprise. See Reverse proxy configuration on page 148. | ✔ | ✔ | ✔ |
| If you are planning to use external clients outside the enterprise firewall, configure client access. See External client access configuration on page 159. | ✔ | ✔ | ✔ |
| Configure an external load balancer. See Route configuration for an external load balancer on page 145. | — | — | ✔ |

# Chapter 4: Planning and preinstallation

Review this chapter before you start installing the Avaya Aura® Web Gateway. You can either deploy the Avaya Aura® Web Gateway using Amazon Web Services (AWS) or VMware.

**Warning:**

When you deploy Avaya Aura® Web Gateway, avoid copying and pasting commands directly from this document. This can introduce unwanted characters and errors. Double-check all inputs you copy or type them manually.

## Planning checklist

This checklist outlines planning requirements and tasks that you must complete before deploying the Avaya Aura® Web Gateway.

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 1 | Ensure that you have all required skills and knowledge. | Before deploying Avaya Aura® Web Gateway, ensure that you have all required skills and knowledge described in this chapter. | |
| 2 | Ensure that you have all required components and equipment. | Team Engagement deployments require Avaya Aura®. Your deployment can also include Conferencing. For more information about components, see Product compatibility on page 21.<br>You must also have:<br>• A virtual machine. You can deploy Avaya Aura® Web Gateway in a VMware or Amazon Web Services environment either using either an Avaya-provided OVA or as a software-only application. Ensure your system meets the specifications outlined in Resource profile specifications for Avaya Aura Web Gateway on VMware on page 30 and Resources profile | |

*Table continues…*

| No. | Task | Notes | ✔ |
|---|---|---|---|
| | | specifications for Avaya Aura Web Gateway on Amazon Web Services on page 31.<br>• The Red Hat Enterprise Linux 7.6 operating system, if you are planning to install Avaya Aura® Web Gateway as a software-only application. If you are installing Avaya Aura® Web Gateway using an Avaya-provided OVA, the operating system is installed automatically.<br>• An SSH tool, such as PuTTY.<br>**Tip:**<br>Configure your SSH tool to properly see lines in the Avaya Aura® Web Gateway configuration utility. For example, in the PuTTY Reconfiguration screen, navigate to **Window** > **Translation** and do the following:<br>- Set **Remote character set** to **Use font encoding**.<br>- Select **Use Unicode line drawing code points**. | |
| 3 | Determine the structure of your deployment. Deployment types are:<br>• A single FQDN with a single data center.<br>• Multiple FQDNs with a single data center.<br>• Multiple data centers. | Consider the following to determine which deployment type you require:<br>• Do you want a single FQDN for all services or a separate FQDN for each service? A single FQDN has some restrictions and requires internal traffic to be routed through the reverse proxy. However, with a single FQDN, you can use a single certificate for all services.<br>• Does your system require a single data center or multiple regionally-distributed data centers? | |
| 4 | Ensure that you can log in to the Avaya Product Licensing and Delivery System (PLDS) to download software and to obtain licences. | Ensure that you have access to PLDS and can download files. Download the Avaya Aura® Web Gateway installation file from PLDS.<br>Avaya Aura® Web Gateway software and enhanced user privileges are licensed capabilities. | |

*Table continues…*

| No. | Task | Notes | ✔ |
|---|---|---|---|
| | | You can access PLDS at http://plds.avaya.com/. | |
| 5 | Obtain the required IP addresses, FQDNs, and certificates. | The IP addresses are used by the interfaces of the different infrastructure components. Certificates are required to ensure secure interaction between solution components. For more information, see Required FQDNs and certificates on page 29. | |
| 6 | If you are planning to deploy a geographically distributed system, review the external load balancer requirements. | See External load balancer requirements on page 33. | |
| 7 | Open the required ports on the firewall. | For detailed information about the ports that must be opened, go to https://support.avaya.com/security, scroll down, and click **Avaya Product Port Matrix Documents**. Navigate to the Avaya Aura® Web Gateway section and then click on the appropriate Port Matrix document for the release to open it. | |

# Required skills and knowledge

Before deploying the product, ensure that you know how to do the following:

- Manage VMware or AWS deployments.
  - For VMware deployments, you must be familiar with virtual machines using vCenter and vSphere.
  - For AWS deployments, you must be familiar with Amazon Machine Images (AMIs) and with the AWS Management console. For a list of supported browsers in AWS, see https://aws.amazon.com/console/faqs/#browser_support.
- Install, deploy, and use key Avaya Aura® components.
- Install, set up, and use the enterprise LDAP directory.
- Use basic Linux commands.

**Related links**

Product compatibility on page 21

# Required FQDNs and certificates

| Required FQDNs | Required certificates |
|---|---|
| In a single FQDN model, you require one FQDN that represents all services. For example: webservices.company.com.<br><br>From the internet, the FQDN resolves to the IP address of the external Avaya SBCE interface. Internally, from the enterprise, it resolves to the IP address of the internal Avaya SBCE interface. | The certificate includes the FQDN and must be signed by a public CA. |
| FQDN for the Avaya Meetings Server Management service. For example: conferencing_management.company.com.<br><br>Internally the FQDN resolves to the virtual IP address of the Avaya Meetings Server Management system.<br><br>In a multiple FQDN deployment, the FQDN resolves externally to the IP address of the external Avaya SBCE interface. | In a single FQDN deployment, the certificate is signed by the System Manager CA.<br><br>In a multiple FQDN deployment, the certificate is signed by a public CA. |
| FQDN for each Web Collaboration Services server IP address. For example: webconference1.company.com, webconference2.company.com and so on.<br><br>Internally, the FQDN resolves to the IP address of the Web Collaboration Services server.<br><br>In a multiple FQDN deployment, the FQDN resolves externally to the IP address of the external Avaya SBCE interface. | In a single FQDN deployment, the certificate for each Web Collaboration Services server is signed by the System Manager CA.<br><br>In a multiple FQDN deployment, the certificate is signed by a public CA. |
| FQDN for the Avaya Aura® Web Gateway portal server virtual IP address. For example: webgateway.company.com.<br><br>Internally, the FQDN resolves to the virtual IP address of the Avaya Aura® Web Gateway portal service.<br><br>In a multiple FQDN deployment, the FQDN resolves externally to the IP address of the external Avaya SBCE interface. | The certificate must include the global services FQDN in the SAN.<br><br>In a single FQDN deployment, the certificate for each server IP address is signed by the System Manager CA.<br><br>In a multiple FQDN deployment, the certificate is signed by a public CA. |
| FQDN for TURN media tunneling. For example: turnmedia.company.com.<br><br>The FQDN resolves to the IP address of the external Avaya SBCE interface used for TURN media. | The certificate is signed by a public CA. |

*Table continues…*

| Required FQDNs | Required certificates |
|---|---|
| FQDN for HTTP media tunneling. For example: media.company.com.<br>The FQDN resolves to the IP address of the external Avaya SBCE interface used for HTTP media tunneling. | The certificate is signed by a public CA. |
| FQDN for the Avaya SBCE management interface. For example: sbce_management.company.com.<br>The FQDN resolves to the IP address for the internal Avaya SBCE interface used for management. | The certificate is signed by the System Manager CA. |

# Virtual machine requirements

## VMware software requirements

The VMware software requirements apply both to OVA-based and software-only deployment options. The following VMware software versions are supported:

- VMware vSphere ESXi 6.0, 6.5, 6.7, and 7.0
- VMware vCenter Server 6.0, 6.5, 6.7 and 7.0

## Resource profile specifications

### Resource profile specifications for Avaya Aura® Web Gateway on VMware

The following section outlines the resource profile specifications for differently sized virtual machines. The virtual machine resource requirements apply both to OVA-based and software-only deployment options.

| Specifications | Profile 1 | Profile 2 | Profile 3 |
|---|---|---|---|
| **vCPU** | 4 | 8 | 16 |
| **CPU reservation** | 4600 MHz | 9200 MHz | 18400 MHz |
| **Memory** | 6 GB | 12 GB | 16 GB |
| **Hard disk** | 132 GB | | |
| **Minimum clock speed** | 2600 MHz | | |

*Table continues…*

| Specifications | Profile 1 | Profile 2 | Profile 3 |
|---|---|---|---|
| **Capacity** | Both of the following:<br>• 1250 Conferencing or Avaya Workplace Client sessions<br>• 1250 Portal Conferencing users | Both of the following:<br>• 2500 Conferencing or Avaya Workplace Client sessions<br>• 2500 Portal Conferencing users | Both of the following:<br>• 5000 Avaya Workplace Client or Conferencing sessions<br>• 5000 Conferencing Portal users |
| **Server type** | Dell R220 or equivalent | | |
| **CPU** | Intel Xeon CPU E5-26700@2.60GHz | | |
| **Physical processor** | 1 | 2 | 4 |
| **Physical core** | 4 | | |
| **NICs** | 1GBPS | | |
| **Load supported** | • 16 Conferencing calls per second.<br>• 12500 Avaya Workplace Client Busy Hour Call Attempts (BHCA).<br>• 20 Portal user requests per second | • 33 Conferencing calls per second.<br>• 25000 Avaya Workplace Client BHCA.<br>• 40 Portal user requests per second | • 50 Conferencing calls per second.<br>• 50000 Avaya Workplace Client BHCA.<br>• 60 Portal user requests per second |

## Resources profile specifications for Avaya Aura® Web Gateway on Amazon Web Services

The following table outlines the profiles created by the CloudFormation template generators. You can use the CloudFormation template generation tool to create a template for the required profile. The template contains the computing and networking resources required for the profile.

These profile specifications apply both to OVA-based and software-only deployment options.

| Profile | Service size | AWS instance type | vCPUs | Memory (GB) |
|---|---|---|---|---|
| Small | 1250 sessions | c4.xlarge | 4 | 6 |
| Medium | 2500 sessions | c4.2xlarge | 8 | 8 |

### Networking considerations for Amazon Web Services

There are some limitations for establishing public internet VPNs and direct connections into AWS. For more information about Amazon VPC Limits, see the AWS documentation at https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html.

**Important:**

Use a direct connection along with a private WAN connection with Service Level Agreement (SLA) measures to ensure that the network quality is appropriate for signaling and voice traffic.

Avaya is not responsible for network connections between AWS and the customer premises.

When you deploy Avaya Aura® Web Gateway in an AWS environment, also deploy a local LDAP server in AWS. This LDAP server is a replica server that synchronizes content from a master LDAP server within the enterprise. To reduce latency for authentication and directory lookup operations, this LDAP server must be collocated with Avaya Aura® Web Gateway in the same AWS region.

### *Connection types*

You can connect applications in a hybrid network on the Amazon VPC in the following ways:

| Connection type | Resource |
|---|---|
| VPN connection | For information about VPN connections, see:<br>https://docs.aws.amazon.com/vpc/ |
| Direct connection | For information about AWS direct connections, see:<br>https://aws.amazon.com/directconnect/. |

# Virtual disk volume specifications

The following table shows the file system layout for systems deployed using Avaya-provided OVAs.

| Disk Volume | Volume size can be increased | Volume Size (GiB) | | | |
|---|---|---|---|---|---|
| | | Disk 1 | Disk 2 | Disk 3 | Disk 4 |
| /boot | No | 0.2 | | | |
| swap | Yes | 8.0 | | | |
| / | Yes | 4.0 | | | |
| /tmp | Yes | 2.8 | | | |
| /var | Yes | 3.0 | | | |
| /var/log | Yes | 2.0 | | | |
| /var/log/audit | Yes | 3.0 | | | |
| /home | Yes | 4.0 | | | |
| /opt/Avaya | Yes | 15.0 | | | |
| /var/log/Avaya | Yes | | 60.0 | | |
| /media/data | Yes | | | 20.0 | |
| /media/cassandra | Yes | | | | 10.0 |
| Total for disk | | 42.0 | 60.0 | 20.0 | 10.0 |

*Table continues…*

| Disk Volume | Volume size can be increased | Volume Size (GiB) | | | |
|---|---|---|---|---|---|
| | | Disk 1 | Disk 2 | Disk 3 | Disk 4 |
| Total disk size | | 132.0 | | | |

# External load balancer requirements

In a geographically distributed deployment, the Avaya Aura® Web Gateway requires an external load balancer that must comply with the following requirements:

| Requirement | Description |
|---|---|
| The HTTP Global Server Load Balancing (GSLB) must route requests basing on the user's location. | The GSLB functionality can be part of the DNS server and not the load balancer. In this case, however, the DNS server must be able to route requests to different locations based on the location of the browser that initiated the request. |
| The HTTP Load balancer must support session affinity. Session affinity means that all requests from the client are always routed to the same server. | • Session affinity is based on cookies.<br>• The reverse proxy inserts a cookie to responses for incoming HTTP requests and routes subsequent requests that contain the same cookie to the same Avaya Aura® Web Gateway server.<br>• This feature is also known as sticky sessions. Do not use IP-based sticky sessions because this might affect load balancing. |
| The HTTP load balancer must support web sockets. | • The load balancer must not block web socket requests and must relay the web socket connections between the client and the server.<br>• HTTP request timeout must be configurable. You must be able to configure the timeout value to the maximum duration of the conference to prevent it from timing out the web socket session. |
| The HTTP load balancer must support URL routing. | The load balancer must be able to route requests to different backends based on the request URL. |
| The HTTP load balancer must support URL rewrite. | The load balancer must be able to modify the URL path of the request based on simple rules to remove or rename parts of the path. |
| The HTTP load balancer must support TLS 1.2. | Some services might not support TLS versions other than 1.2. |

*Table continues…*

| Requirement | Description |
|---|---|
| The HTTP load balancer must support at least some of the listed ciphers when interacting with back-end services. | • ECDHE-RSA-AES128-GCM-SHA256<br>• ECDHE-ECDSA-AES128-GCM-SHA256<br>• ECDHE-ECDSA-AES256-GCM-SHA384<br>• ECDHE-RSA-AES128-SHA256<br>• ECDHE-ECDSA-AES128-SHA256<br>• ECDHE-RSA-AES128-SHA<br>• ECDHE-ECDSA-AES128-SHA<br>• AES128-GCM-SHA256<br>• AES256-GCM-SHA384<br>• AES128-SHA |
| The HTTP load balancer must be able to use TCP health checks. | The load balancer must be able to perform health checks of Avaya Aura® Web Gateway servers using TCP responses. To avoid leaving multple TCP sockets opened, you must be able to configure TCP health checks to half-opened connections. |
| The external HTTP load balancer must be able to use standard headers to determine the FQDN from the original request that is used to reach the system. | Avaya Aura® Web Gateway uses the “Host” header to identify the FQDN that is used by the client to reach the system.<br>**Note:**<br>This behavior is required if the customer requires different FQDNs per location or uses different FQDNs to reach the system. If a single global FQDN is used, you can ignore this requirement. |
| The external HTTP load balancer must relay the client certificates. | This requirement is only needed for authenticating clients using a client certificate. |
| The HTTP load balancer must be able to insert custom headers to HTTP requests. | |

# Linux alias commands

Linux aliases are defined to make frequently used commands easier to use. When an alias is available for the required operation, you can use the alias instead of typing a long path name and using `sudo`. The path name specification and `sudo` invocation are built into the aliases that Avaya provides.

**Table 1: Three categories of aliases with their functionality description**

| Alias | Description |
|---|---|
| `cdto` | Change to frequently used directories. |

*Table continues…*

| Alias | Description |
|---|---|
| app | Perform application functions, such as install or backup. |
| svc | Manage the state of application related services. |

Some of the alias commands are only available after the application has been installed.

You can type any of the aliases in a Linux shell to list the supported commands.

The following image provides an example of how the aliases are used:

```
[admin@aawg-ova ~]$ cdto

Syntax: cdto <target>

Available navigation targets:

    base            [/opt/Avaya]
    root            [/opt/Avaya/CallSignallingAgent]
    active          [/opt/Avaya/CallSignallingAgent/3.4.0.0.299]
    cas             [/opt/Avaya/CallSignallingAgent/3.4.0.0.299/CAS/3.4.0.0.299]
    misc            [/opt/Avaya/CallSignallingAgent/3.4.0.0.299/CAS/3.4.0.0.299/misc]
    bin             [/opt/Avaya/CallSignallingAgent/3.4.0.0.299/CAS/3.4.0.0.299/bin]
    config          [/opt/Avaya/CallSignallingAgent/3.4.0.0.299/CAS/3.4.0.0.299/config]
    logs            [/opt/Avaya/CallSignallingAgent/3.4.0.0.299/CAS/3.4.0.0.299/logs]
    ilogs           [/opt/Avaya/CallSignallingAgent/.CSAInstallLogs]
    tlogs           [/opt/Avaya/CallSignallingAgent/3.4.0.0.299/tomcat/8.0.24/logs]

[admin@msg-esg ~]$ app

Syntax: app <command> <arguments>

Available commands:

    install         [Run application installer for installation]
    status          [statusCSA.sh]
    configure       [configureCSA.sh]
    listnodes       [clitool-csa.sh listClusterNodes]
    collectlogs     [collectLogs.sh]
    backup          [backupCSA.sh]
    restore         [restoreCSA.sh]
    upgrade         [Run application installer for upgrade]
    rollback        [rollbackCSA.sh]
    removeinactive  [removeVersion.sh (inactive instance)]
    uninstall       [uninstallCSA.sh]
```

Each alias category displays the target command, which is in square brackets. The syntax for the command is provided in the procedures outlined in this document. Arguments that you specify after an alias are passed through to the target command.

The system can simultaneously have both an active and inactive installation of the software. For example, after an upgrade, the earlier version becomes inactive, but the new version becomes active. The alias commands operate only on the active installation unless specified.

**Table 2: Examples of alias commands to be used in a Linux shell**

| Alias example | Function provided |
|---|---|
| `cdto logs` | Changes to the log directory of the active installation on the system. |
| `app install` | Runs the staged application installer. |
| `svc telportal restart` | Restarts the telportal service. |

**Note:**

The aliases must be used only from the command line in a Linux shell. Do not use them in a script. You must use the actual target command in a script.

# System layer commands

The **sys** command line alias facilitates the use and discovery of system layer commands. Typing this command without arguments provides syntax help, and a list of supported system layer commands. The following is an example:

```
[admin@server-dev ~]$ sys

Execute system layer commands.

    -h, --help
        Command syntax (this help)

    -hh, --hhelp
        Verbose help

Available commands:

    secconfig       [Manage security settings]
    versions        [Query version information]
    volmgt          [Manage disk volume sizes]
    smcvemgt        [Manage Spectre/Meltdown patches]
    extension       [Manage system layer extensions]
  passwdrules     [Manage password rules]

  Command invocation syntax:
     sys <command> <arguments>

  Command syntax
    sys <command> -h

[admin@server-dev ~]$
```

## Verbose help information

**-hh** is used for verbose help information, which provides a brief description of each available system layer command. The following is an example:

```
[admin@server-dev ~]$ sys -hh

The "sys" command line alias facilitates access to the following commands
related to the system layer of UCApp appliances. To obtain help with
each of these commands, use the "-h" (or "--help") argument for help
```

```
with command line syntax, and "-hh" (or "--hhelp") for verbose help.

secconfig
    Manages security-related settings.

versions
    Queries the version information of various elements of the system
    layer.

volmgt
    Queries the sizes of existing disk volumes and extends their sizes.

smcvemgt
    Manages the enablement status of Linux kernel patches for the
    Spectre and Meltdown vulnerabilities.

extension
     Manages the extensions for the system layer. Supported extensions
     are currently limited to the enablement of JAR files in the
     JRE library's extensions directory to support newer application
    loads.

[admin@server-dev ~]$
```

Any arguments provided after the name of the system layer command are passed through to that command.

## sys secconfig command

**`sys secconfig`** provides access to the **`secconfig`** command, which existed in previous releases. The following is an example of this command:

```
[admin@server4950csa ~]$ sys secconfig --hhelp

This script is used to manage run-time security settings on this appliance.
The following command-line arguments are available:

    --help, -h
        Prints terse help (command line syntax).

    --hhelp, -hh
        Prints verbose help (this help).

    --sshCBC < --enable | --disable | --query >
    -cbc     < -e       | -d        | -q >
        Enables, disables, and queries the current state of SSH daemon
        CBC-based ciphers.

   --fips  < --enable | --disable | --query >
   Enables, disables, and queries the current state of FIPS on the system.

[admin@server4950csa ~]$
```

# sys versions command

The **sys versions** command provides a summary of key system layer information, including the type of appliance (OVA), the version number of the system layer, the version of the current partitioning, and the OVA that was originally deployed.

```
[admin@server4889csa ~]$ sys versions

    Appliance type       : AAWG
    System layer version : 3.4.3.0.2
    Partitioning version : 2.0
    Original OVA deploy  : csa-3.5.0.0.365

[admin@server4889csa ~]$
```

# sys volmgt command

## Syntax help: sys volmgt --help

The **sys volmgt** command is used to query and extend disk volumes on the system.

**Important:**

The **sys volmgt** command is only available if data encryption is *disabled* on Avaya Aura® Web Gateway. If data encryption is enabled, this command is unavailable and you cannot allocate free disk space to disk volumes.

The following provides the command line syntax for this command:

```
[admin@server4889csa ~]$ sys volmgt --help

Syntax:
    --help,                  -h
    --hhelp,                 -hh
    --version,               -v
    --status,                -st
    --summary,               -s
    --monitor  [tail|less],  -m [tail|less]
    --logs,                  -l
    --scan
    --extend <volume> [ <n>m | <n>g | <n>t --remaining ]
  --extend --all
    --reset

[admin@server4889csa ~]$
```

## Verbose help: sys volmgt --hhelp

The verbose help information for the scripts provides more information about what the tool is used for.

```
[admin@server4889csa ~]$ sys volmgt --hhelp

This script provides for the ability to extend the sizes of volumes on this
system. In order for a volume to be extended in size, the disk that hosts
the volume must first be increased in size using the tools that are used
to manage deployed virtual machines (VMware).
```

```
The following example illustrates how to add 20 GiB of storage to the
application log volume (/var/log/Avaya). This volume is located on the second
disk of the system and so this example assumes that disk 2 has been increased
in size by 20 GiB.

    sys volmgt --extend /var/log/Avaya 20g

The above example will do two things:

    1) It will extend the size of the LVM logical volume by 20 GiB.

    2) It will then extend the size of the Linux file system that is
       located inside that volume to the new size of the LVM logical
       volume.

Step (2) above may take several minutes to complete for larger volumes. If,
for some reason, this second operation is interrupted, it can be re-run
using the same command, but WITHOUT specifying the size argument. For example,
the following command is used to perform step (2) only for the application
log volume (/var/log/Avaya).

    sys volmgt --extend /var/log/Avaya

If in doubt as to whether or not all file systems have been fully extended in
their respective volumes, step (2) can be executed across all volumes using
a single command as follows:

    sys volmgt --extend --all

Performing step (2) on a file system that is already fully extended in its
LVM volume is a null operation (does no harm).

Note the following general points regarding this script:

- The extending of a volume cannot be undone. Make sure the correct volume
  is being extended, and by the correct size. To confirm any extend
  operation, the user is required to enter the response "confirm"
  (case insensitive).

- In order to avoid impacting system performance, avoid performing extend
  operations during periods of high traffic.

- Extend operations are performed by a background process, in order to
  avoid interference due to loss of an SSH connection. Avoid powering down
  or rebooting a server while there is a background operation in progress.
  The presence of a running background operation can be queried as follows:

    sys volmgt --status

- Logical volumes on the system are referenced using their Linux file system
  mount points, such as /var/log/Avaya and /media/data, with the exception
  of the volume containing Linux swap, which has no mount point. The Linux
  swap volume is referenced using "swap".

- Sizes are specified in base 2 units rather than base 10 (SI) units. For
  example, 1g = 1 GiB = 1024 x 1024 x 1024 bytes.

- Summary information is displayed in GiB, with a resolution of two decimal
  places. When extending the sizes of LVM volumes, units can be specified
  in mebibytes (m), gibibytes (g), or tebibytes (t).

- Due to file system overhead allocation by the Linux kernel, the size
  of a file system will never exactly match the size as reported by
  the LVM volume that contains that file system. To be certain that a file
  system is fully extended to the size of the volume that contains it,
```

```
  inspect the log file after issuing the extend operation as follows:

      sys volmgt --monitor less

  To perform such a check across all volumes:

      sys volmgt --extend --all
      sys volmgt --monitor less

The following arguments are supported by this script:

    --help, -h
        Terse help.

    --hhelp, -hh
        Verbose help (this help).

    --version, -v
        Prints the version of this script to stdout.

    --status, -st
        Prints the current status of this tool. Use this to determine
        if there is a background operation in progress, or the results
        of the last background operation.

    --summary, -s
        Prints a summary of disks, the LVM volumes contained on each disk,
        and the file system contained in each LVM volume. Disk information
        includes the size of the disk and the amount of free space
        available for allocation to volumes on the disk. LVM volume
        information includes the size of the LVM volume. File system
        information includes the size of the Linux file system and the
        current amount of space that is in use on that file system.

        Due to file system overhead allocation by the Linux kernel, the
        size of a file system will never exactly match the size as reported
        by the LVM volume that contains that file system. Refer to the top of
        this help information for more information.

    --monitor [tail|less]
    -m        [tail|less]
        Browse the log file for the latest extend operation. Specify "tail"
        to use the tail browser. Specify "less" to use the less
        browser, which allows scrolling and searching through the log file.
        If neither is specified, the browser defaults to the tail browser.

    --logs
        Generate a zip file in the current working directory that contains
        all logs generated to date by this script.

    --scan
        Scan disks for newly available storage. Do this after increasing
        the disk size of one of more disks. Once scanned, the newly
        available space appears in the "Free" column in the "--summary"
        output, and is now available for allocation to volumes on that disk.

        A summary is printed after the scan to show the updated volume
        information.

    --extend <volume> [ <n>m | <n>g | <n>t --remaining ]--extend --all
        The first form of the command operates on a single volume. If a size
        is specified, then the LVM volume is extended by that size (step 1),
        and the file system it contains is extended to use the new space
        made available in that volume (step 2). If a size is not specfied,
        then the file system contained in that volume is extended (i.e.,
```

```
        step 2 only).

        The "--all" form of the command is used to perform step 2 across
        all volumes on the system.

        For more information, see the examples at the top of this help.

        If "--remaining" is specified for the size, then the specified
        volume is extended with all remaining free space on that disk.
        If a specific increment is provided, then the volume is extended
        by that amount, reducing the amount of free space on the disk
        by that amount. Specific sizes are in the form of a number
        (e.g., "10", "10.5", or ".5") and a unit. Units are "m" for
        mebibites, "g" for gibibytes", and "t" for tebibytes".

        The smallest increment that can be specified is 100 MiB.

        Example invocations:

            sys volmgt --extend /var/log/Avaya 10g
            sys volmgt --extend /var/log/Avaya 10.5g
            sys volmgt --extend /var/log/Avaya 0.5g
            sys volmgt --extend /var/log/Avaya .5g
            sys volmgt --extend /var/log/Avaya 500m
            sys volmgt --extend /var/log/Avaya --remaining
            sys volmgt --extend /var/log/Avaya

  --reset
        Resets internal tracking data. Use this if this script is blocked
        on an invalid background progress indication. This condition can
        arise if a background operation was prematurely terminated due to,
        for example, a system reboot. Verify that no background operations
        are in progress prior to executing this command, through verification
        of the process id as reported by the "--status" argument.

[admin@server4889csa ~]$
```

## Partitioning examples: sys volmgt --summary

Avaya Aura® Web Gateway supports partitioning version 2.0.

The following example shows a summary of the information provided by this command for a version 2.0 partitioned system:

```
[admin@server4950csa ~]$ sys volmgt -s

                          Disk and Volume Summary

+----------- Disk ------------+------------------- Volume --------------------+
|                              |                      LVM        File System    |
| Num  Name     Size     Free |    Name              Size      Size     Usage |
+------------------------------+-----------------------------------------------+
|  1   sda      41.78    0.00 | /                     4.00      3.81      1.26 |
|                              | /home                 4.00      3.81      0.05 |
|                              | /opt/Avaya           14.97     14.61      1.14 |
|                              | /tmp                  2.81      2.71      0.01 |
|                              | /var                  3.00      2.89      0.03 |
|                              | /var/log              2.00      1.91      0.00 |
|                              | /var/log/audit        3.00      2.89      0.00 |
|                              | swap                  8.00       n/a       n/a |
+------------------------------+-----------------------------------------------+
|  2   sdb      60.00    0.00 | /var/log/Avaya       60.00     58.93      0.05 |
+------------------------------+-----------------------------------------------+
|  3   sdc      20.00    0.00 | /media/data          20.00     19.56      0.04 |
+------------------------------+-----------------------------------------------+
```

```
|  4    sdd       10.00     0.00 | /media/cassandra     10.00       9.71       0.02 |
+-----------------------------+-------------------------------------------------+
```

# sys smcvemgt command

The system layer **smcvemgt** command is used to manage the Linux kernel patches related to the following vulnerabilities:

- Variant #2/Spectre (CVE-2017–5715)
- Variant #3/Meltdown (CVE-2017–5754)

**Note:**

The kernel patch for the Variant #1/Spectre (CVE-2017–5754) vulnerability is permanently enabled on the system and cannot be disabled.

The choice to enable or disable these patches is a trade-off between performance and security impact:

- If the patches are enabled, the system might experience noticeable performance losses.
- If the patches are disabled, the system is not protected against the Variant #2/Spectre and Variant #3/Meltdown vulnerabilities.

By default, Linux patches for Variant #2/Spectre and Variant #3/Meltdown are enabled. The Variant #2/Spectre patch is enabled with Linux kernel defaults. In default operation mode, the Variant #2/Spectre Linux patch selects the mitigation method that is best suited for the processor architecture of the host machine.

**Note:**

To be fully functional, patches for the Variant #2/Spectre vulnerability require hardware support, which is provided by VMware and hardware vendors through microcode updates.

Changes made by the **smcvemgt** command to the Linux kernel tunalbles always cause a server reboot. The script does not manage the state of application services. To ensure that the application services are stopped before the reboot, run the `svc csa stop` command before using the **smcvemgt** command. After the reboot, manually start the application services using the `svc csa start` command.

For more information about Spectre and Meltdown kernel tunables that are affected by the **smcvemgt** command, see https://access.redhat.com/articles/3311301. For more information about the Spectre and Meltdown vulnerabilities, see https://access.redhat.com/security/vulnerabilities/speculativeexecution.

### Syntax help: sys smcvemgt --help

```
[admin@server-dev ~]$ sys smcvemgt --help

Version 1.2

Syntax:
    --help,    -h
    --hhelp,   -hh
    --query,   -q
    --set,     -s  enabled
    --set,     -s  disabled
    --set,     -s  [ v2=<v2-mode> ] [ v3=<v3-mode> ]
```

```
        (v2-mode: disabled | default | kernel | user | both | user+retp)
        (v3-mode: disabled | enabled)
    --history
```

## Verbose help: sys smcvemgt --hhelp

```
[admin@srvr-dev ~]$ sys smcvemgt --hhelp

Version 1.2

This script manages the enablement status of the Linux kernel patches for the
following Spectre and Meltdown vulnerabilities:

    Variant #2/Spectre  (CVE-2017-5715)
    Variant #3/Meltdown (CVE-2017-5754)

The kernel patch for the following related vulnerability is permanently enabled
on the system (cannot be disabled):

    Variant #1/Spectre (CVE-2017-5753)

Note that hardware support is required for Variant #2/Spectre to be fully
functional. CPU microcode updates must be applied in order for this hardware
support to be provided. The "--query" argument includes an indication as to
whether or not hardware support is provided on this server.

For more information on Spectre/Meltdown kernel tunables, refer to:

    https://access.redhat.com/articles/3311301

For additional information on the Spectre/Meltdown vulnerabilities, refer
to:

    https://access.redhat.com/security/vulnerabilities/speculativeexecution

Syntax:

    --help,    -h
        Provide terse help.

    --hhelp,   -hh
        Provide verbose help (this text).

    --query,   -q
        Query the configuration of the Variant #2/Spectre and Variant #3/
        Meltdown tunables for system reboots, as well as on the running
        system.

    --set,  -s  enabled
    --set,  -s  disabled
    --set,  -s  [ v2=<v2-mode> ] [ v3=<v3-mode> ]
        Enables and disables Variant #2/Spectre ("v2") and/or Variant #3/
        Meltdown ("v3") patches.

        This immediately reboots the server. Applications on the server are
        not managed by this script. Ensure that any applications are
        disabled, as required, prior to changing kernel settings with this
        script.

        If "enabled" is specified, then both v2 and v3 are enabled,
        with v2 set to kernel default behavior. If "disabled" is specified,
        then both v2 and v3 are disabled. Otherwise, kernel patches
        are enabled or disbled as per the specified "v2" and/or "v3"
        arguments. If a "v2" or "v3" argument is not specified, the current
        system value for that item is retained.
```

```
        v2-mode:

            disabled
                Variant #2/Spectre is disabled.

            default
                The kernel decides how to set tunables for Variant #2/
                Spectre, based on the processor architecture. Note that for
                architectures prior to Skylake, the kernel selects
                retpoline ("return trampoline") over ibrs.

            kernel
                Use "ibrs" (i.e., kernel space only).

            user
                Use "ibrs_user" (i.e., userland only).

            both
                Use "ibrs_always" (i.e., kernel space and userland).

            user+retp
                Use "retpoline,ibrs_user".

        v3-mode:

            disabled
                Variant #3/Meltdown is disabled.

            enabled
                Variant #3/Meltdown is enabled.
        The following two commands are equivalent:

            sys smcvemgt enabled
            sys smcvemgt v2=default v3=enabled

        The following two commands are equivalent:

            sys smcvemgt disabled
            sys smcvemgt v2=disabled v3=disabled

    --history
        Show a history of changes made to the enablement status of the
        Spectre and Meltdown patches.
```

# sys smcvemgt usage examples

## Command for querying current tunable settings

The following command queries the current tunable settings for the next boot, as well as the current runtime. This command also indicates whether there is hardware support for Variant #2/Spectre.

```
sys smcvemgt --query
```

## Command for enabling patches with default settings

The following command enables patches for Variant #2/Spectre and Variant #3/Meltdown, where Variant #2/Spectre is configured for default mode. In default mode, the kernel selects the Variant #2/Spectre mitigation mechanism based on the CPU architecture of the host machine.

```
sys smcvemgt --set enabled
```

### Commands for enabling patches with specific settings

- The following command enables patches for Variant #2/Spectre and Variant #3/Meltdown, where Variant #2/Spectre is set to kernel space only.

```
sys smcvemgt --set v2=kernel v3=enabled
```

- The following command enables patches for Variant #2/Spectre, which are configured for user space with “Retpoline”, or “return trampoline”. Variant#3/Meltdown retains its current settings.

```
sys smcvemgt --set v2=user+retp
```

### Command for disabling patches

The following command disables patches for Variant #2/Spectre and Variant #3/Meltdown.

```
sys smcvemgt --set disabled
```

### Command for disabling patches for a specific vulnerability

The following command disables patches for Variant #3/Meltdown. Variant #2/Spectre retains its current settings.

```
sys smcvemgt --set v3=disabled
```

## passwdrules command

### Description

**sys passwdrules** allows you to review and edit complexity rules for passwords that you use to log in to the virtual machine with the Avaya Aura® Web Gateway OVA using an SSH connection.

If data encryption is enabled, these rules also apply to encryption passphrases.

### Syntax

```
sys passwdrules [show] [set [options]] [set-default]
```

| | |
|---|---|
| **show** | Shows the server password rule configuration, including default, minimum, and maximum values. |
| **set** | Sets server password rules. If you do not specify any options, then Avaya Aura® Web Gateway prompts you to configure each option separately. If you do not specify a certain option, Avaya Aura® Web Gateway continues to use the existing rule for this option. |
| **set-default** | Sets server password rules to their default values. |

### Syntax help

```
sys passwdrules [-h | --help]
```

### Options

| Option | Description |
|---|---|
| `--diff=`*`INTEGER`* | Number of characters in the new password that must not be present in the old password. |
| `--min-len=`*`INTEGER`* | Minimum length of the password. |
| `--min-digs=`*`INTEGER`* | Minimum number of digits in the password. |
| `-min-upper=`*`INTEGER`* | Minimum number of uppercase characters in the password. |
| `--min-lower=`*`INTEGER`* | Minimum number of lowercase characters in the password. |
| `--min-other=`*`INTEGER`* | Minimum number of special characters in the password.<br>**Important:**<br>Avaya Aura® Web Gateway supports the following special characters: !, @, #, %, $, ^, *, ?, and _. |
| `--min-class=`*`INTEGER`* | Minimum number of character classes that must be present in the password. The character classes are:<br>• Digits<br>• Uppercase characters<br>• Lowercase characters<br>• Special characters |
| `--max-repeat=`*`INTEGER`* | Maximum allowed number of consecutively repeated characters.<br>For example, if you set this parameter to 3, then the following password is invalid: `paaassword`, because `a` is repeated three times. |
| `--max-class-repeat=`*`INTEGER`* | Maximum allowed number of consecutively repeated characters of the same class.<br>For example, if you set this parameter to 3, then the `pas1sw2or3d` password is invalid, because the first three characters, which are `p`, `a`, and `s`, belong to the same character class. |

### Example

The following is an example of a command that sets the following password rules:

- At least 16 characters in total.
- At least two digits.
- At least one special character.
- Other settings are default.

```
sys passwdrules set --min-len=16 --min-digs=2 --min-other=1
```

# Data encryption commands

The following sections contains command you can use to manage data encryption. These commands are available if you enabled data encryption during Avaya Aura® Web Gateway OVA deployment.

You cannot enable or disable data encryption using system layer commands.

**Important:**

In AWS deployments, you enable data encryption on AWS itself. Therefore, you cannot use the system layer commands for disk encryption management in AWS deployments.

## encryptionPassphrase command

### Description

You can run the **sys encryptionPassphrase** command to manage the encryption passphrase.

### Syntax

```
sys encryptionPassphrase [add | change | remove | list]
```

| | |
|---|---|
| **add** | Enables you to set up an encryption passphrase. |
| **change** | Enables you to change the existing encryption passphrase. |
| **remove** | Removes the encryption passphrase. |
| **list** | Displays information about passphrases and slot assignments. |

## encryptionRemoteKey command

### Description

You can use the **sys encryptionRemoteKey** command to manage the remote key server. If you run the command without any parameters, Avaya Aura® Web Gateway displays help information about the command.

### Syntax

```
sys encryptionRemoteKey [add <server address> [<port>] | remove <server address> | list]
```

| | |
|---|---|
| **add** | Enables you to add a remote key server. |
| **remove** | Removes the remote key server. |
| **list** | Displays general remote key server information. |

## encryptionLocalKey command

### Description

You can use the **disk encryptionLocalKey** command to manage the local key store. If you run this command without any parameters, Avaya Aura® Web Gateway displays help information.

### Syntax

```
sys encryptionLocalKey [enable | disable]
```

| | |
|---|---|
| **enable** | Enables the local key store. |
| **disable** | Disables the local key store. |

## encryptionStatus command

### Description

The **sys encryptionStatus** command displays information about data encryption on Avaya Aura® Web Gateway , including the following:

- Whether data encryption is enabled.
- Whether the local key store is enabled.
- Whether the encryption password is used.

### Syntax

```
sys encryptionStatus
```

# Characters supported for Avaya Aura® Web Gateway passwords

You can use the following characters for Avaya Aura® Web Gateway passwords:

- Uppercase letters: A to Z
- Lowercase letters: a to z
- Numerics: 0 to 9
- Special characters: !, @, #, %, $, ^, *, ?, and _

These rules apply to all passwords that you enter manually to access resources and for Keystore passwords.

**Note:**

The web administration portal supports Active Directory-based authentication. Therefore, you can use other special characters, such as double quotes ("), for web administration portal passwords.

# Chapter 5: Initial setup for VMware and AWS deployments

You can use the following options to deploy Avaya Aura® Web Gateway:

- As a software-only application that you can install on your own Red Hat Enterprise Linux (RHEL) 7.6 physical servers or virtual machines.
- In a VMware environment using an Avaya-provided, application-specific RHEL 7.6 OVA.

  This option also includes installing Avaya Aura® Web Gateway on an Appliance Virtualization Platform host using Solution Deployment Manager.
- In an Amazon Web Services (AWS) environment using an Avaya-provided, application-specific RHEL 7.6 OVA.

Use the following sections to perform the initial VMware or AWS setup.

## Deployment process checklist

This checklist describes the high-level deployment process for virtual machine deployments on VMware and AWS.

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 1 | Depending on the deployment option, do one of the following:<br>• For OVA-based deployments, Deploy the OVA for VMware or AWS environment.<br>• For software-only deployments, deploy your RHEL 7.6 virtual machines and install the system layer. | If you deploy Avaya Aura® Web Gateway using an Avaya-provided OVA, see:<br>• For VMware deployments, see the procedures in VMware deployments on page 51.<br>• For Amazon Web Services deployments, see the procedures in Amazon Web Services deployments on page 57. | |

*Table continues…*

| No. | Task | Notes | ✔ |
|---|---|---|---|
| | | If you deploy Avaya Aura® Web Gateway as a software-only application, see:<br>• For VMware deployments, see the procedures in Software-only installation checklist for VMware-based environment on page 74.<br>• For Amazon Web Services deployments, see the procedures in Software-only installation checklist for Amazon Web Services on page 85.<br>The Avaya Aura® Web Gateway OVA file includes openjdk. Operating system updates for virtual machines include updates for openjdk. | |
| 2 | Optional: Enable FIPS mode. | For OVA-based deployments, you can only enable FIPS mode before installing the application layer. For information about enabling FIPS for OVA-based deployments, see Enabling FIPS mode on page 94.<br>For software-only deployments, you can only enable FIPS mode before installing the system layer. For information about enabling FIPS for software-only deployments, see Enabling FIPS for software-only systems on page 80. | |
| 3 | Optional: For OVA-based deployments, enable additional STIG hardening. | You only need to enable additional hardening if your organization policies require full Security Technical Implementation Guide (STIG) compliance.<br>For more information, see Enabling additional STIG hardening on page 96.<br>You cannot enable additional STIG hardening in software-only deployments. | |
| 4 | Install or restore the application layer as required. | For information about installing the initial node, see Installing the Avaya Aura Web Gateway on page 98.<br>For information about installing additional nodes, see Installing | |

*Table continues…*

| No. | Task | Notes | ✔ |
|---|---|---|---|
| | | additional nodes to create a cluster on page 104. | |
| 5 | If you are installing a cluster, configure RSA keys for SSH connections after all additional nodes are installed. | See Configuring RSA public and private keys for SSH connections in a cluster on page 107. | |

# VMware deployments

Deploy the Avaya Aura® Web Gateway OVA on a virtual machine using either vCenter or vSphere. The components of the Avaya Aura® Web Gateway, Endpoint Service Gateway, and Unified Portal are provided in a single OVA file.

## Obtaining the Avaya Aura® Web Gateway OVA file

### Procedure

Do one of the following:

- Download the Avaya Aura® Web Gateway OVA from the Avaya Product Licensing and Delivery System (Avaya PLDS) at https://plds.avaya.com.
- Place an order for the DVDs containing the OVA file using the Material Code ID or description.

  For more information about the material ID, see “Product Order Codes and Pricing” in *Avaya Aura® Web Gateway Offer Definition*.

## OVA deployment

Use one of the following procedures to deploy the OVA. You can use vCenter, vSphere, or Solution Development Manager (SDM).

**Important:**

When deploying an Avaya Aura® Web Gateway cluster, you must use the same resource profile for each Avaya Aura® Web Gateway node in the cluster. Mixed profile clusters are not supported.

**Related links**

Resource profile specifications for Avaya Aura Web Gateway on VMware on page 30

## Supported vSphere clients

The following table lists vSphere clients that you can use to deploy the Avaya Aura® Web Gateway OVA depending on the VMware ESXi version you are using.

| Client type | Launched from | Is supported on | | |
|---|---|---|---|---|
| | | ESXi 6.0 | ESXi 6.5 | ESXi 6.7 |
| vSphere client application | Application installed on your computer. | ✔ | ✖ | ✖ |
| vSphere web client for vCenter | Web client launched with the IP of vCenter. | ✔ | ✔ | ✔ |
| ESXi host web client | Web client launched with the IP of the individual ESXi host. | ✔ | ✔ | ✔ |

# Deploying the Avaya Aura® Web Gateway OVA using vCenter

## Procedure

1. Log in to vCenter.
2. Navigate to **File** > **Deploy OVF Template**.
3. From the Source page, click **Browse** and then select the OVA file.

   For example, `csa-<version>_OVF10.ova`
4. Verify the information displayed in OVF Template Details and then click **Next**.
5. Review and accept the End User License Agreement (EULA) and then click **Next**.
6. From the Name and Location page, do the following:
   a. Specify a name.
   b. Select an inventory location or data store.
   c. Click **Next**.
7. From the Deployment Configuration page, select a profile and then click **Next**.

   You can select one the following resource profiles from the **Configuration** drop-down menu:

   - AAWG Profile 3 Max Sessions 5,000
   - AAWG Profile 1 Max Sessions 1,250
   - AAWG Profile 2 Max Sessions 2,500

   If you are deploying the OVA for a non-seed node in a cluster, you must use the same resource profile that you used for the seed node. For more information about resource profile specifications, see Resource profile specifications for Avaya Aura Web Gateway on VMware on page 30.
8. From the Host/Cluster page, do the following:
   a. Select the host on which the template will be deployed.

b. Click **Next**.

9. From the Disk Format page, do the following:
   a. Select a thick or thin provision option.

      If you select a thick provision option, the entire disk space will be reserved and unavailable for other virtual machines to use.

      If you select the thin provision option, unused space will be available for other virtual machines to use.

   b. Click **Next**.
10. From the Network Mapping page, do the following:
   a. Map the source network used with the appropriate destination network.
   b. Click **Next**.
11. From the Properties page, do the following:
   a. Complete the required network information, such as your IP address, host name or FQDN, Netmask, and DNS.
   b. Enter credentials for a Linux administrator user, which include the user name, password, and group.

      The default user name is `admin`, group is `admingrp`, and password is `avaya123`.

   c. Configure data encryption settings.

      For information about data encryption fields, see Data encryption field descriptions on page 53.
12. From the Ready to Complete tab, verify your settings and then click **Next** to complete the installation.

### Next steps

Install the Avaya Aura® Web Gateway.

## Data encryption field descriptions

Data encryption is only supported with AVP and the VMware Virtualized Environment.

| Name | Description |
|---|---|
| **Data Encryption** | Use this option to enables or disable data encryption.<br>The options are:<br>• **1**: To enable data encryption.<br>• **2**: To disable data encryption. |

*Table continues…*

| Name | Description |
|---|---|
| | **Important:**<br>You cannot change encrypted Avaya Aura® Web Gateway to non-encrypted or vise versa without a new OVA installation.<br>• On Solution Deployment Manager: When the **Data Encryption** field is set to 1, Avaya Aura® Web Gateway enables the **Encryption Pass-Phrase** and **Re-enter Encryption Pass-Phrase** fields to enter the encryption passphrase.<br>• On vCenter or ESXi: When the **Data Encryption** field is set to 1, enter the encryption passphrase in the **Password** and **Confirm Password** fields. |
| **Encryption Pass-Phrase** | The passphrase for data encryption. This field is applicable when data encryption is enabled.<br>When you deploy Avaya Aura® Web Gateway using Solution Deployment Manager, Avaya Aura® Web Gateway applies the password complexity rules.<br>When you deploy Avaya Aura® Web Gateway using vCenter or ESXi, Avaya Aura® Web Gateway does not apply password complexity rules.<br>**Important:**<br>While using vCenter, when you enable data encryption and do not enter the encryption passphrase, the system does not block the deployment due to a vCenter limitation. Therefore, ensure that you enter the encryption passphrase if data encryption is enabled. |
| **Re-enter Encryption Pass-Phrase** | The password for data encryption. |
| **Require Encryption Pass-Phrase at Boot-Time** | When this check box is selected, you must type the encryption passphrase whenever Avaya Aura® Web Gateway reboots. By default the **Require Encryption Pass-Phrase at Boot-Time** check box is selected.<br>**Important:**<br>You must remember the data encryption passphrase. If you lose the data encryption password, the only option to access Avaya Aura® Web Gateway is to reinstall the OVA.<br>If the check box is not selected, Avaya Aura® Web Gateway creates a local key store and you do not need to type the encryption passphrase when Avaya Aura® Web Gateway reboots. However, this will make the system less secure.<br>You can also set up a remote key server and start using it by running the **`sys encryptionRemoteKey`** command after Avaya Aura® Web Gateway is installed. The remote key server provides more security than the local key store. |

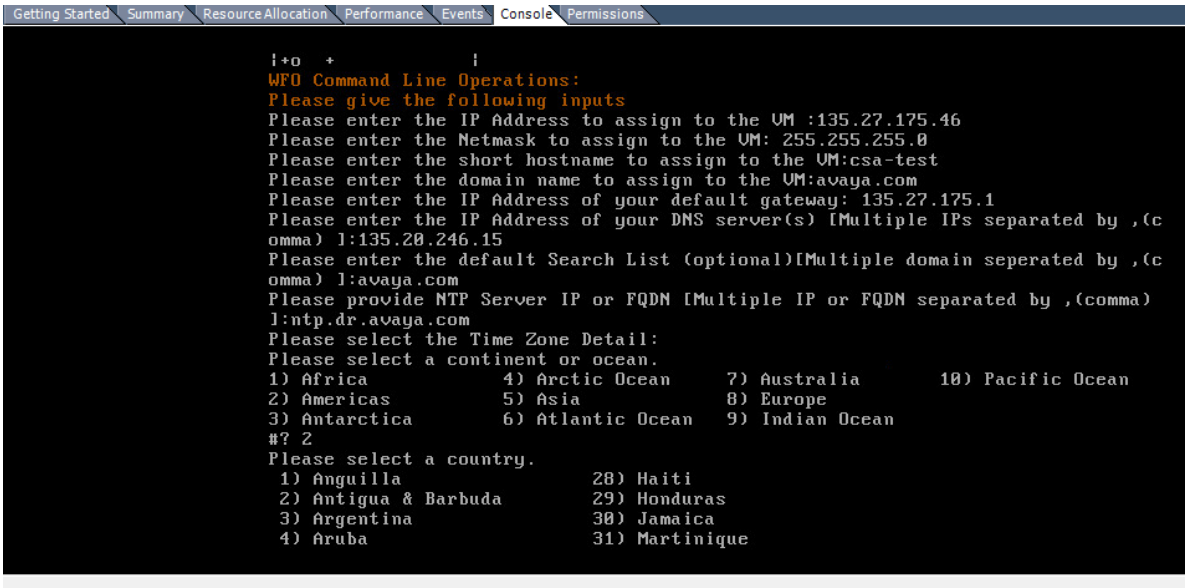
# Deploying the Avaya Aura® Web Gateway OVA using vSphere connected directly to the ESXi host

## Procedure

1. Log in to vSphere.
2. Navigate to **File** > **Deploy OVF Template**.
3. Perform steps 3 on page 52 to 9 on page 53.

   These steps are the same in vCenter and vSphere.
4. Turn on your virtual machine, and do the following:
   a. Access the VM console.
   b. Accept the license agreement and continue with the following post-installation steps.
5. Provide the network settings information

   The following image provides an example of network and IP settings in the VM console:




6. Ensure that the Default Search List includes the list of domains for:
   - Avaya Aura® Web Gateway
   - Avaya Meetings Server Management
   - System Manager and LDAP

# Deploying the Avaya Aura® Web Gateway OVA through Solution Deployment Manager from System Manager

## About this task

Use this procedure to create a virtual machine on the ESXi host and deploy the Avaya Aura® Web Gateway OVA on the virtual machine. You can also use this procedure to deploy the Avaya Aura® Web Gateway OVA on Appliance Virtualization Platform (AVP).

## Before you begin

- Ensure that you are familiar with the “Deployment checklist” section in *Deploying Avaya Aura® applications from System Manager*.
- Add AVP or an ESXi host to the location. For more information, see “Adding an Appliance Virtualization Platform or ESXi host” in *Deploying Avaya Aura® applications from System Manager*.

## Procedure

1. Upload the required OVA file to System Manager.

   For information about uploading a file to the software library, see “Downloading the OVA file to System Manager” in *Deploying Avaya Aura® applications from System Manager*.
2. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
3. In **Application Management Tree**, select a platform.
4. On the Virtual Machines tab, in the VMs for Selected Location <location name> section, click **New**.

   The system displays the VM Deployment window.
5. In the Select Location and Platform section, do the following:
   a. In **Select Location**, select a location.
   b. In **Select Platform**, select a platform.

      The system displays the hostname in the **Platform FQDN** field.
6. In **Data Store**, select a data store.
7. Click **Next**.
8. On the OVA tab, do the following:
   a. In **Select Software Library**, select **Select OVA from software library**.
   b. In **Select Software Library**, select the local or remote library where the OVA file is located.
   c. In **Select OVAs**, select the OVA that you want to deploy.
   d. In **Flexi Footprint**, select the footprint size that the application supports.

9. On the Configuration Parameters page, specify the following:
   - Management network settings
   - Public network settings
   - Admin user details
10. On the Network Parameters page, choose any application.
11. Click **Deploy**.
12. Click **Accept the license terms**.

    In the Hosts for Selected Location <location name> section, the system displays the deployment status in the Current Action Status column.

    The system displays the virtual machine on the VMs for Selected Location <location name> page.
13. To view details, click **Status Details**.

# Amazon Web Services deployments

Amazon Web Services (AWS) is a cloud services platform that enables enterprises to securely run applications on the virtual cloud. The key components of AWS are Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3).

When you deploy Avaya Aura® Web Gateway in an AWS environment, also deploy a local LDAP server in AWS. This LDAP server is a replica server that synchronizes content from a master LDAP server within the enterprise. To reduce latency for authentication and directory lookup operations, this LDAP server must be collocated with Avaya Aura® Web Gateway in the same AWS region.

AWS deployments *do not* support IPv6.

**Note:**

Use the AWS Command Line Interface (CLI) for managing AWS services from your computer. For more information about setting up the AWS CLI, see https://aws.amazon.com/cli and http://docs.aws.amazon.com/cli/latest/userguide/cli-chap-getting-started.html#cli-quick-configuration.

**Note:**

Use Elastic IP addresses for AWS deployments. An Elastic IP address is a public IPv4 address, which is reachable from the Internet. If your instance does not have a public IPv4 address, you can associate an Elastic IP address to enable communication with the internet. For example, you can connect to the instance from your local computer. For more information about elastic IPs, see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html.

# Signing in to the AWS Management console

## About this task

There are many different ways you can sign in to your AWS account, so step-by-step procedures are not given here. See the following website for more information:

https://aws.amazon.com/premiumsupport/knowledge-center/sign-in-console/

## Before you begin

Ensure that you have an AWS account.

# Configuring AWS details using the AWS CLI

## About this task

The first time that you use the AWS CLI, you must configure the AWS details.

## Before you begin

Set up the AWS CLI on a computer with access to AWS. For more information, see http://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html.

## Procedure

1. Start a command line interpreter on the computer with the installed AWS CLI.

   **Note:**

   The AWS CLI supports different Windows and Linux command line interpreters, such as PowerShell or Bash.

2. From the command line interpreter, run the command `aws configure`, and do the following:
   a. For **AWS Access Key ID**, type the AWS access key ID.
   b. For **AWS Secret Access Key**, type the AWS secret access key ID.
   c. For **Default region name**, type the region name.

      For example: `us-west-2`.

   d. For **Default output format**, type `text` or `json`.

# Creating a key pair

## About this task

A key pair is a set of public and private keys. The public key is used to encrypt data, such as the login password. The private key is used to decrypt the encrypted data. You provide this key pair

when you create a CloudFormation stack, and use it for SSH access to the Amazon Machine Instances.

For more information, see the following website:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html

### Procedure

1. Sign in to the Amazon Web Services Management console.
2. In the left navigation pane, go to **NETWORK & SECURITY**, and click **Key Pairs**.
3. Click **Create Key Pair**.
4. In the Create Key Pair dialog box, in the **Key pair name** field, type a name for the key pair.
5. Click **Create**.

   The system generates a `*.pem` file and prompts you to save the file on your computer. You can also view the created key pair name in the Key pair name column.
6. Save the `*.pem` file.

   **Important:**

   When you create a key pair, save it. If you lose the key, you cannot retrieve it and you will not be able to access the instance.

# OVA to AMI conversion

## Creating a bucket for uploading the OVAs for AMI conversion

### Procedure

1. Sign in to the Amazon Web Services Management console.
2. Under **AWS services**, navigate to **All services** > **Storage** > **S3**.

   The system displays the S3 Management Console page.
3. Click **Create bucket**.

   The system displays the Create bucket dialog box.
4. In **Bucket name**, type a unique bucket name.

   Only use lowercase letters for the name.
5. In the **Region** field, click a region for your bucket.
6. Click **Create bucket**.

### Next steps

Upload the Avaya Aura® Web Gateway OVA.

## Creating a service role

### About this task

Use this procedure to create a role named `vmimport` for importing files into the S3 bucket.

Use the AWS CLI to run the commands in this procedure.

### Procedure

1. Start a command line interpreter on a computer with the installed AWS CLI.
2. Run the following command to create a role named `vmimport` and let the AWS image import service assume this role:

   ```
   aws iam create-role --role-name vmimport --assume-role-policy-document <file://
   trust-policy.json>
   ```

   In this command, `<file://trust-policy.json>` is a path to the `trust-policy.json` file. This file is included in the AWS configuration files artifact.
3. Open the `role-policy.json` file, and in each `"Resource": "arn:aws:s3:::<disk-image-file-bucket>"` string, replace `<disk-image-file_bucket>` with the actual S3 bucket name.

   For example:

   ```
   "Resource": "arn:aws:s3:::my-s3-bucket"
   ```
4. Run the following command to allow the `vmimport` role to perform importing procedures:

   ```
   aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-
   document <file://role-policy.json>
   ```

   In this command, `<file://rule-policy.json>` is a path to the `rule-policy.json` file. This file is included in the AWS configuration files artifact.

## Uploading the Avaya Aura® Web Gateway OVA

### Before you begin

Download the OVAs from the Avaya PLDS website at http://plds.avaya.com/.

### Procedure

1. Sign in to the Amazon Web Services Management console.
2. Under **AWS services**, navigate to **All services** > **Storage** > **S3**.

   The system displays the S3 Management Console page.
3. From the All Buckets area, select a bucket.
4. Click **Upload**.
5. In the dialog box that is displayed, click **Add Files** and upload the Avaya Aura® Web Gateway OVA with the `-aws-001-ova` suffix.

# Converting the imported OVA to AMI

## About this task

You can use files in the JSON format that are included in the AWS configuration files artifact. The AWS configuration files artifact also contains single-node and multi-node CloudFormation template generators that you use for AWS server deployment. The AWS configuration file contains the following:

- `trust-policy.json`
- `role-policy.json`
- `Single-Node-Cloud-Template-Gen.html`
- `Multi-Node-Cloud-Template-Gen.html`

For more information, see http://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html.

Use the AWS CLI to run the commands in this procedure.

## Before you begin

You need the following to convert the OVA file to an Amazon Machine Image (AMI), to deploy the AMI, and configure Avaya Aura® Web Gateway:

- Avaya Aura® Web Gateway OVAs with the `-aws-001.ova` suffix has been uploaded to an S3 bucket.

Ensure that you also convert the `*.pem` file to the `*.ppk` format and configure PuTTY for establishing an SSH connection.

Ensure that you updated AWS details using the AWS CLI. For more information, see Configuring AWS details using the AWS CLI on page 58.

## Procedure

1. Start a command line interpreter on a computer with the installed AWS CLI.
2. Run the following command to check whether the S3 bucket is ready to use:

   ```
   aws s3 ls
   ```

   The system displays the S3 bucket that you created.
3. To view the content of the S3 bucket, run the `aws s3 ls s3://<nameofbucket>` command.
4. To import the ova for conversion, run the following command:

   ```
   >aws ec2 import-image --cli-input-json "{ \"Description\": \"<server.ova>\",
   \"DiskContainers\": [ { \"Description\": \"<text description of task>\",
   \"UserBucket\": { \"S3Bucket\": \"<your_bucket_name>\", \"S3Key\" : \"<server.ova>
   \" } } ]}"
   ```

   The system displays the Status and the ImportTaskId parameters.

   In the following example, when the system converts the CM Simplex OVA, ImportTaskId is `import-ami-ffmanv5x`.

   ```
   {
       "Status": "active",
   ```

```
    "Description": "<version>-aws-001.ova",
    "Progress": "2",
    "SnapshotDetails": [
        {
            "UserBucket": {
                "S3Bucket": "<version>-dev",
                "S3Key": "<version>-aws-001.ova"
            },
            "DiskImageSize": 0.0
        }
    ],
    "StatusMessage": "pending",
    "ImportTaskId": "import-ami-fftlelct"
}
```

5. To check the status of the import image, run the following command:

   ```
   aws ec2 describe-import-image-tasks --cli-input-json "{ \"ImportTaskIds\":
   [\"<Your_ImportTaskId>\"], \"NextToken\": \"abc\", \"MaxResults\": 10 } "
   ```

   The conversion process takes up to 30 minutes. You can run the above command repeatedly.

   In the following example, the process is preparing the AMI and is 76% complete:

   ```
   IMPORTIMAGETASKS x86_64 CM-Simplex-07.1.0.0.xxx-aws-001.ova import-ami-ffgji45r
   BYOL Linux 76 active preparing ami
   ```

   The output format varies depending on the selection of the text or JSON format on the AWS CLI configuration.

6. Sign in to the Amazon Web Services Management console.
7. Go to **Services** > **Compute** and then click **EC2**.

   The system displays the EC2 Management Console page.

8. In the left navigation pane, click **IMAGES** > **AMIs**.

   You can search the converted AMI with ImportTaskId. The system displays the newly converted AMI ImageId in the AMI ID column.

### Next steps

Create CloudFormation templates, which can be used to create a stack.

# Creating CloudFormation templates

### About this task

Use CloudFormation templates to create an AWS stack.

**Important:**

To create CloudFormation templates, use one of the following web browsers:

- Google Chrome
- Mozilla Firefox

Internet Explorer and Microsoft Edge are *not* supported.

### Before you begin

Download the compressed artifact containing the configuration files to your computer. Extract the two CloudFormation generator HTML files from the compressed file.

- To create a single-node CloudFormation template, do the following:
  1. In your web browser, to run the template generator, open the `Single-Node-Cloud-Template-Gen.html` file.
  2. In **Product**, select the required application and profile size.
  3. In **Instance Type**, select the required instance type.
  4. Click **Generate template**.
  5. Save the file to your computer.
- To create a multi-node CloudFormation template, do the following:
  1. In your web browser, run the template generator by opening the `Multi-Node-Cloud-Template-Gen.html` file.
  2. In **Product**, select the required application and profile size.
  3. In **Instance Type**, select the required instance type.
  4. In **Number of nodes**, set the number of servers required for the cluster.
  5. In **Number of subnets**, set the number of subnets required for the cluster.

     You can set two or three subnets.
  6. Do one of the following:
     - To create new subnets for availability zones, select the **Create subnets** check box.
     - If you are planning to use the existing subnets, clear the **Create subnets** check box.
  7. Click **Generate template**.
  8. Save the file to your computer.

### Next steps

Deploy the CloudFormation stack:

- For a single-node system, see Deploying a single-node CloudFormation stack on page 63.
- For a multi-node system, see Deploying a multi-node CloudFormation stack on page 67.

## Deploying a single-node CloudFormation stack

### About this task

Use this procedure to deploy a standalone instance by using a single-node CloudFormation template.

### Before you begin

- Use standard Amazon Web Services procedures to create the required network setup, including Virtual Private Cloud (VPC) settings and Security Groups.
- Generate a single-node CloudFormation template.
- Ensure that you have network access to the Amazon VPC before deploying an AMI.

### Procedure

1. Sign in to the AWS console and navigate to **Services** > **Management & Governance** > **CloudFormation**.

   CloudFormation is an AWS service used to create a stack. A stack is a graph of objects such as EC2 instances and EBS volumes inside the Amazon cloud. CloudFormation is used to create the objects required for a single-node Avaya Aura® Web Gateway system within a subnet of an existing virtual network.

2. On the CloudFormation page, click **Create Stack**.
3. On the Create Stack page, click **Select Template**.
4. When the template is ready, click **Upload a template file**.
5. Select the single-node `yaml` CloudFormation template file that you generated.
6. Click **Next**.
7. On the Specify Details page, in the **Stack name** field, type the stack name.

   The hostname for the node is derived from the stack name.

   **Note:**

   The stack name must start with a letter and must contain letters, numbers, and dashes.

8. In **Amazon Machine Image ID**, type the Amazon Machine Image ID (AMI ID) of the instance you created.

   For example, `ami-fda9369d`.

   **Tip:**

   To obtain the AMI ID of an image, go to **Services** > **EC2** > **Images** > **AMIs** .

9. In the Network area, select the required **Virtual Private Cloud** and **Subnet**.
10. In **DNS domain**, type the name of the private DNS domain to use.

    This domain name represents the domain name that clients use to access the service.

11. If the domain is a new domain in this VPC, set **Create domain** to **Y**. Otherwise, set it to **N**.
12. In the Security area, select **SSH key for administrator login**.
13. Click **Next**.
14. **(Optional)** On the Options page, in the Tag area, add tags to help you find and organize the AWS objects.

15. In the Permissions area, leave the default values for **IAM Role** and **Enter role arn**.
16. Click **Next**.
17. On the Review page, confirm the stack information.
18. Click **Create** to create the stack.

    The system displays the Stacks page, which shows the stack creation status.
19. Wait until the status displays `CREATE_COMPLETE`.

    You can monitor the stack creation status and review the properties using the tabs at the bottom of the Stacks page.
20. Click the **Resources** tab.
21. Click the Physical ID of the EC2 instance for the node. For example, `i-0fccb4a222a32dcc9`.

    The system displays the Instances page using a filter that displays the newly created AMI.
22. **(Optional)** Click the **Actions** menu to change the instance state.

    For example, you can start, stop, or reboot the AMI virtual machine.

### Next steps

To complete the first-login configuration, log in to the EC2 instance using the “admin” user name and the private key that you used when creating the CloudFormation stack.

**Related links**

Logging in to the EC2 instance on page 72
Completing the first-login configuration on page 72

# AWS cluster deployments

Use the information in the following subsections for multi-node AWS clusters.

For traffic distribution, use the AWS load balancer. A virtual IP address for clusters is not available on AWS.

**Important:**

When deploying an Avaya Aura® Web Gateway cluster, you must use the same resource profile for each Avaya Aura® Web Gateway node in the cluster. Mixed resource profile clusters are not supported.

## Creating and applying load balancer certificates

### About this task

Load balancers only appear in the private DNS within AWS. Therefore, certificates generated by external certificate authorities might not work. Use this procedure to obtain a certificate from System Manager within AWS.

### Procedure

1. On the System Manager web console, navigate to **Home** > **Services** > **Security** > **Certificates** > **Authority**.
2. Click **Add End Entity** and complete the settings in the following fields:
   a. **End Entity Profile**: Type `<INBOUND_OUTBOUND_TLS>`.
   b. **Username**: Type `<FQDN of the load balancer>`.

      The FQDN of the load balancer is the service FQDN of the cluster. This domain name portion of the FQDN represents the domain name that clients use to access service. The FQDN must be the combination of the stack name followed by the domain. For example, if the stack name is `yourStack` and the domain is `your.domain.com`, then the FQDN is `yourStack.your.domain.com`.

      **Note:**

      The stack name must start with a letter and must contain only letters, numbers, or dashes. This stack name must be used during multi-node CloudFormation.
   c. **Password**: Type your password.
   d. **Confirm Password**: Retype your password.
   e. **CN, Common name**: Type `<FQDN of the load balancer>`.
   f. **Token**: Select the `PEM` file.

      **Note:**

      The remaining fields are optional. For more information, see *Administering Avaya Aura® System Manager*.
3. Click **Add**.
4. Navigate to **Home** > **Services** > **Security** > **Certificates** > **Authority** > **Public Web**.

   The system displays the EJBCA public page.
5. Click **Create Keystore**.
6. In **Username**, type the FQDN of the load balancer.
7. In **Password**, type the End Entity password that you created earlier.
8. Click **OK**.

   The system displays the EJBCA Token Certificate Enrollment page.
9. In **Key length**, select the required key length.

   A length of 2048 bits is recommended.
10. Click **Enroll** and select a text editor to view the certificate.
11. Save the `PEM` file to your computer.
12. Sign in to the AWS console and navigate to **Services** > **Security, Identity & Compliance** > **Certificate Manager**.

13. Click **Import a certificate**.

    The system displays a form with three fields: **Certificate Body**, **Certificate private key**, and **Certificate chain**.

14. Open the `PEM` file you saved earlier with a text editor and do the following:

    **Note:**

    You must include the BEGIN and END labels for each section that you paste into the form.

    a. In the Private Key section, copy the string from `-----BEGIN PRIVATE KEY-----` to `-----END PRIVATE KEY-----` and paste it into the **Certificate private key** field.

    b. In the Certificate section, copy the first certificate string from `-----BEGIN CERTIFICATE-----` to `-----END CERTIFICATE-----` and paste it into the **Certificate body** field.

    c. In the Certificate section, copy the second certificate string from `-----BEGIN CERTIFICATE-----` to `-----END CERTIFICATE-----` and paste it into the **Certificate chain** field.

15. Click **Review and import**.

16. Click **Import**.

    The system imports the certificate and displays the status and details of the certificate.

17. Copy and save the ARN value in the Details section.

    The ARN is required for the **Load balancer certificate ARN** field during the multi-node CloudFormation deployment.

## Deploying a multi-node CloudFormation stack

### About this task

Use multi-node CloudFormation to create a cluster.

**Note:**

You cannot expand an AWS single node into an AWS cluster. Create AWS clusters from the beginning. However, after an AWS cluster is created, it can be expanded. For more information, see Expanding an existing cluster on page 69.

### Before you begin

- Use standard Amazon Web Services procedures to create the required network setup, including Virtual Private Cloud (VPC) settings and Security Groups.
- Ensure that you have network access to the Amazon VPC before deploying an AMI.
- Create a multi-node CloudFormation template as described in Creating CloudFormation templates on page 62.
- Create and apply load balancer certificates. The ARN value created during the certificate import is required for this procedure.

### Procedure

1. Sign in to the Amazon Web Services Management console.
2. Navigate to **Services** > **Management & Governance** > **CloudFormation**.
3. Click **Create Stack**.

   The AWS EC2 Management console displays the first page of the Create stack wizard.
4. When the template is ready, click **Upload a template file**.
5. Select the multi-node `yaml` CloudFormation template file you generated.
6. Click **Next**.

   The system displays the Specify Details page.
7. In **Stack name**, type a name for the stack.

   This stack name must match the stack name portion of the FQDN of the load balancer.
8. In **Amazon Machine Image ID**, type the Amazon Machine Image ID (AMI ID) of the image you imported.

   For example, `ami-fda9369d`.

   **Tip:**

   You can obtain the AMI ID of an image from the EC2 AMI page. On a separate browser tab, navigate to **Services** > **EC2** > **Images** > **AMIs**.
9. In the Network area, select the required **Virtual Private Cloud**.
10. Do one of the following depending on whether you select the **Configure subnets** check box in step 2 on page 63 when creating the multi-node CloudFormation template:

    - If you select the check box, configure the required IPv4 address range in each subnet CIDR block field.

      In CIDR notation, the number of bits in the network portion of the address follows a slash. For example, 10.143.11.192/28. The address range for the subnets must fall within the address range of the VPC and must not overlap any existing subnet within the VPC.
    - If you did not select the check box, select the required subnets from each **Subnet** field.

      **Note:**

      When using existing subnets, each subnet must be in a different availability zone.
11. In **DNS domain**, type the name of the private DNS domain to use.

    This domain name must match the domain name used in the FQDN of the load balancer.
12. If the domain is a new domain in this VPC, set **Create domain** to **Y**.

    Otherwise, set it to **N**.
13. In the Security area, select **SSH key for administrator login**.

14. Copy the ARN saved in the Details section and paste it into the **Load balancer certificate ARN** field.

    For information on copying the ARN, see Creating and applying load balancer certificates on page 65.

15. Click **Next**.

    The system displays the Options page.

16. **(Optional)** In the Tags area, add tags to help you find and organize the AWS objects.
17. In the Permissions area, keep the default values for both **IAM Role** and **Enter role arn**.
18. Click **Next**.

    The system displays the Review page.

19. Click **Create** to create the stack.

    The system displays the Stacks page, which shows the stack creation status.

20. Wait until the status displays `CREATE_COMPLETE`.

    You can monitor the stack creation status and review the properties using the tabs at the bottom of the Stacks page.

21. Click the **Resources** tab.
22. Click the Physical ID of the EC2 instance for the node. For example, `i-0fccb4a222a32dcc9`.

    The system displays the Instances page using a filter that displays the newly created AMI.

23. **(Optional)** Click the **Actions** menu to change the instance state.

    For example, you can start, stop, or reboot the AMI virtual machine.

### Next steps

To complete the first-login configuration, log in to the EC2 instance using the “admin” user name and the private key that you used when creating the CloudFormation stack.

**Related links**

Logging in to the EC2 instance on page 72
Completing the first-login configuration on page 72

## Expanding an existing cluster

### About this task

An existing AWS cluster can be expanded with additional nodes by updating the stack that represents the cluster.

**Note:**

You cannot expand a single AWS node into an AWS cluster. You must create AWS clusters from the beginning.

### Procedure

Add nodes to a cluster by updating the CloudFormation stack that represents the cluster.

## Creating a hybrid cloud for client access

### About this task

Servers deployed in AWS are contained within a Virtual Private Cloud (VPC). End user clients are present within a separate network but require access to the servers in AWS. You must create a VPN to enable client access.

You must configure VPN gateways at both ends of the tunnel:

- The address range assigned to the VPC must route to the gateway on your side of the tunnel.
- Within AWS, the address range that clients use must route to the AWS-side gateway.

Use this procedure to configure AWS so that the address range that clients use routes to the AWS-side of the gateway.

### Before you begin

- Deploy the required EC2 instances.
- Assign an IP address range to the VPC that does not overlap with any subnet in your network.

### Procedure

1. Sign in to the AWS console.
2. Navigate to **Services** > **Management Tools** > **CloudFormation** and select the required stack.
3. Click the **Resources** tab.
4. Click the physical ID link for one of the nodes.

   The system displays a page with the details of the node.
5. Copy the value from the **Subnet ID** field of the Description tab. For example, `subnet-99942eff`.
6. Navigate to **Services** > **Networking & Content Delivery** > **VPC** > **Subnets**.
7. Paste the subnet ID into the **Search Subnets** filter.
8. Select the subnet that the system displays.
9. Select the row that contains the previously noted ID in the Route Table ID column.
10. Select the **Route Table** tab.
11. Click the route table ID link that is located next to the **Edit** button. For example, `rtb-bc53a2db`.

12. Select the route that the system displays.
13. Select the Routes tab.
14. Click **Edit**.
15. Click **Add another route** to add each required client address range and do the following:
    a. In the Destination column, enter the address range.
    b. In the Target column, select an AWS-side gateway that can reach the destination.
16. Click **Save**.

# Configuring on-premise DNS resolution of VPC addresses

### About this task

This configuration allows on-premise clients to access the servers hosted in the AWS VPC. Use this procedure to configure your local, on-premise DNS server with a new DNS forwarding zone so that client DNS resolution requests are forwarded to a DNS server located within the VPC. The DNS server located within the VPC then performs the final address resolution to the servers hosted in the AWS VPC.

### Before you begin

Ensure that you have:

- Access to your on-premise DNS server so that you can add a new DNS forwarding zone.
- Enabled your corporate firewall to permit outgoing UDP traffic toward the AWS VPC.
- Routes on your AWS VPC VPN gateway that direct UDP port 53 traffic from the enterprise toward the VPC.
- The IP address of the DNS server in the AWS VPC.
- A list of the VPC domains that the on-premise DNS server must resolve to the AWS DNS server. For example, if your VPC servers must resolve `server.example.com` and `server.example.net`, then the list of required VPC domains is `example.com` and `example.net`.
- A test FQDN that is configured in the VPC DNS.

### Procedure

1. Log on to your local on-premises DNS server.
2. Add a new “Forward Zone” or “Forward Lookup Zone” DNS by following the instructions provided by your DNS server manufacturer.
3. Add a new forward zone with the following details for each required VPC domain:
    a. A zone name: Use the same name as the domain name. For example, `example.com`.
    b. The forwarding address: Use the IP address and port of the DNS server in the AWS VPC. For example, `10.1.2.3@53`.

c. Forward First: Enable Forward First if your DNS server supports this feature. This feature causes resolution requests for the zone to be forwarded to the VPC DNS server before attempting to resolve them locally.

4. Enable the DNS server changes by reloading the configuration or restarting the DNS server.
5. Verify that the DNS resolution completes by performing a lookup of the test FQDN using a DNS resolution utility, such as `nslookup` or `dig`.

   For example, you can run the following `nslookup` command:

```
>  nslookup server.example.com
Server:          192.168.0.1
Address:         192.168.0.1#53

Non-authoritative answer:
Name:    server.example.com
Address: 10.1.2.165
```

# Logging in to the EC2 instance

## Procedure

Log in to the EC2 instance using the SSH console or PuTTY.

**Important:**

- Use the “admin” user name to log in to the instance.
- You must use the private key from the key pair that you used during CloudFormation stack creation. If you use PuTTY, the key must be in the `.ppk` format.

  When you use the private key, you do not need to enter a password to access the EC2 instance.

For information about configuring and using PuTTY, see Connect to your Linux instance from Windows using PuTTY.

# Completing the first-login configuration

## About this task

The first time you access a newly deployed EC2, you must complete a one-time system procedure to accept the license agreement, configure the OS, and select network preferences.

## Before you begin

- Ensure that you use the private key from the key pair that you used during CloudFormation stack creation to establish the an SSH connection.

  If you use PuTTY, the private key must be in the `.ppk` format.
- Access the EC2 instance by logging in using PuTTY or SSH from the command line. To access the instance, use the IP address of the instance.

### Procedure

1. When prompted to enter the user name, enter `admin`.
2. Do the following when you see the license agreement banner, which is displayed when you log in for the first time:
   a. Press `Enter` to display the license agreement.
   b. Press the `Space bar` to navigate through the license agreement.
   c. When prompted, type `yes` to accept the license agreement.
3. To configure the NTP servers, do one of the following:
   - Press `Enter` to accept the default Amazon NTP time servers.
   - Enter one or more comma separated NTP server IP addresses or FQDNs and then press `Enter`.

   **Important:**

   The NTP servers that you configure must be reachable from this server. The default Amazon NTP time serves are on the Internet and might not be reachable.
4. Select your time zone preferences.
5. Review the summary of your selections and type one of the following:
   - `y`: To apply the settings to the system.
   - `n`: To make changes to your selections.

### Next steps

Install the Avaya Aura® Web Gateway application software using the `app install` command as described in Installing the Avaya Aura Web Gateway on page 98.

Complete the required configuration and commissioning procedures after the initial installation. If you are installing a cluster, you must follow the instructions for using an external load balancer.

# Software-only deployments

You can deploy Avaya Aura® Web Gateway as a software-only application using your own virtual or physical machines and Red Hat Enterprise Linux 7.6. Avaya Aura® Web Gateway supports the following deployment options:

- VMware virtualization environment. Avaya Aura® Web Gateway supports the following platforms:
  - ESXi: Releases 6.0, 6.5, 6.7, and 7.0.
  - Appliance Virtualization Platform (AVP): Releases 8.1.2 and 8.1.3.
- Amazon Web Services (AWS) virtualization environment.

- Physical servers.

After installing and configuring the operating system, you must install the system layer on virtual machines. After that, use the common installation, configuration, and administration tasks to complete the Avaya Aura® Web Gateway deployment.

# Software-only deployment in VMware-based virtualization environment

## Software-only installation checklist for VMware-based environment

The following checklist outlines the tasks that you must perform when deploying Avaya Aura® Web Gateway as a software-only application on your own physical servers or in VMware-based environment.

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 1 | Ensure that virtual machines that you plan to use to deploy Avaya Aura® Web Gateway comply with the requirements for software-only installation. | See the requirements in VMware software requirements on page 30 and Resource profile specifications for Avaya Aura Web Gateway on VMware on page 30. | |
| 2 | Download the Avaya Aura® Web Gateway software-only installation package from PLDS. | The software-only installation package includes the following files:<br>• Software-only system layer installer.<br>• Avaya Aura® Web Gateway application installer.<br>The package file name has the `csa-swonly-<AAWG_VERSION>.tgz` format. | |
| 3 | Install Red Hat Enterprise Linux (RHEL) 7.6. | Avaya Aura® Web Gateway Release 3.9 requires RHEL 7.6. For more information about installation, see the official Red hat documentation. Avaya also recommends that you install the latest security updates on RHEL. | |
| 4 | Create disk partitioning on RHEL. | Avaya Aura® Web Gateway requires specific disk partitioning to organize data storage. For more information about creating disk partitioning, see Creating disk partitioning for software-only deployments on page 76 and Disk partitions for software-only deployments on page 76. | |

*Table continues…*

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 5 | Create a non-root Linux user. | The installation and administration of the Avaya Aura® Web Gateway server is more secure when performed by non-root users with sudo privileges. For more information, see Creating administrative users on page 78. | |
| 6 | Enable the YUM package manager on RHEL. | The YUM package manager is used to install the required packages. For more information about enabling YUM, see the Red Hat YUM documentation. | |
| 7 | Enable FIPS mode (optional). | For software-only deployments, you can only enable FIPS mode before installing the system layer. For more information, see Enabling FIPS for software-only systems on page 80, Additional packages required for FIPS mode on page 81, and Enabling the Haveged service on page 82. | |
| 8 | Do one of the following to manage additional RHEL packages:<br>• Register your RHEL instance to the Red Hat subscription.<br>• Create a local repository for RPM installation or updates. | For more information, see RHEL packages management on page 79.<br>Registering your RHEL instance to the Red Hat subscription is the preferred option. | |
| 9 | Install the software-only system layer on your RHEL. | The system layer is low-level software that forms the required operational environment for Avaya Aura® Web Gateway.<br>For more information, see Installing the system layer on page 82. | |
| 10 | Ensure that:<br>• NTP service is up and running.<br>• System Manager is reachable from your virtual machine. | Perform these checks to ensure that the system layer is installed successfully so you can install the Avaya Aura® Web Gateway application.<br>For more information, see Checking the NTP service status on page 84 and Checking the connection to System Manager on page 84. | |

## Red Hat Enterprise Linux installation

When you deploy Avaya Aura® Web Gateway as a software-only solution, you must use the Red Hat Enterprise Linux (RHEL) 7.6. For details about obtaining and installing RHEL 7.6, see the Red Hat website https://www.redhat.com.

After obtaining RHEL 7.6, do the following:

1. Install the RHEL 7.6 operating system by using the Red Hat installation procedures.

   **Important:**

   Avaya Aura® Web Gateway requires specific disk partitioning. You can create the required data disks and physical volumes for data disks during or after RHEL 7.6 installation using the values provided in Disk partitions for software-only deployments on page 76.

2. Install the latest critical security updates.

   For update procedures, see Red Hat documentation. You can install security updates by using the YUM package manager.

### Disk partitions for software-only deployments

The following table shows Avaya Aura® Web Gateway disk partitions and their logical volumes with appropriate sizes:

| Disk | Disk size (GB) | Mount Point |
|---|---|---|
| Disk 1:<br>• `/dev/sda` for VMware<br>• `/dev/xvda` for AWS | 42 | – |
| Disk 2:<br>• `/dev/sdb` for VMware<br>• `/dev/xvdb` for AWS | 60 | `/var/log/Avaya` |
| Disk 3:<br>• `/dev/sdc` for VMware<br>• `/dev/xvdc` for AWS | 20 | `/media/data` |
| Disk 4:<br>• `/dev/sdd` for VMware<br>• `/dev/xvdd` for AWS | 10 | `/media/cassandra` |

## Creating disk partitioning for software-only deployments

### About this task

Avaya Aura® Web Gateway requires a specific disk layout that includes several disk partitions and logical volumes. Use this procedure to create appropriate disk partitioning.

### Before you begin

- Create physical volumes with the required disk size values. For more information, see Disk partitions for software-only deployments on page 76.

Install RHEL on virtual machines.

## Procedure

1. Log in to the virtual machine as the root user using an SSH connection.
2. Run the following commands to create the required directories:

```
mkdir -p /var/log/Avaya
mkdir -p /media/data
mkdir -p /media/cassandra
```

3. Depending on your virtual environment, do the following to create the required physical volumes and volume groups for these volumes:
   - In a VMware virtual environment, run the following commands:

```
pvcreate -f /dev/sdb
vgcreate disk2_vg /dev/sdb
pvcreate -f /dev/sdc
vgcreate disk3_vg /dev/sdc
pvcreate -f /dev/sdd
vgcreate disk4_vg /dev/sdd
```

   - In an virtual AWS environment, run the following commands:

```
pvcreate -f /dev/xvdb
vgcreate disk2_vg /dev/xvdb
pvcreate -f /dev/xvdc
vgcreate disk3_vg /dev/xvdc
pvcreate -f /dev/xvdd
vgcreate disk4_vg /dev/xvdd
```

4. Run the following commands to create logical volumes in the volume groups:

```
lvcreate -l100%FREE -n application_log /dev/disk2_vg
lvcreate -l100%FREE -n data /dev/disk3_vg
lvcreate -l100%FREE -n cassandra /dev/disk4_vg
```

5. Run the following commands to create a file system for the `/dev/sdb` partition and mount the file system:

```
mkfs.xfs /dev/disk2_vg/application_log
mount /dev/disk2_vg/application_log /var/log/Avaya
echo "/dev/disk2_vg/application_log /var/log/Avaya xfs defaults 0 0" >> /etc/fstab
```

6. Run the following commands to create file systems for the `/dev/sdc` partition and mount the file system:

```
mkfs.xfs /dev/disk3_vg/data
mount /dev/disk3_vg/data /media/data
echo "/dev/disk3_vg/data /media/data xfs defaults 0 0" >> /etc/fstab
```

7. Run the following commands to create file systems for the `/dev/sdd` partition and mount the file system:

```
mkfs.xfs /dev/disk4_vg/cassandra
mount /dev/disk4_vg/cassandra /media/cassandra
echo "/dev/disk4_vg/cassandra /media/cassandra xfs defaults 0 0" >> /etc/fstab
```

# Creating administrative users

## About this task

You must use a non-root Linux user with sudo privileges to install the Avaya Aura® Web Gateway application. The User ID (UID) of the Linux user that performs the installation must be the same on all nodes in the cluster.

This procedure describes how to add users and groups. For a clustered deployment of Avaya Aura® Web Gateway, perform the steps described in this procedure on every node in the cluster.

## Before you begin

Deploy Red Hat Enterprise Linux (RHEL) 7.6 on virtual machines.

## Procedure

1. Log in to the virtual machine with deployed RHEL 7.6 as the root user using an SSH connection.
2. Run the following command to create a group for the administrative user:

   ```
   groupadd -g 4001 <admin_group>
   ```

   In this command, `<admin_group>` is a group name of your choice. For example:

   ```
   groupadd -g 4001 admingrp
   ```

   **Important:**

   For Group ID (GID), you must use `4001`.

3. Run the following command to add an administrative user in the new administrative group:

   ```
   useradd -g <admin_group> -u 4001 <admin_name>
   ```

   In this command, `<admin_group>` is the name of the group you created in the previous step, and `<admin_name>` is an administrative user name of your choice. For example:

   ```
   useradd -g admingrp -u 4001 aadsadmin
   ```

   **Important:**

   For User ID (UID), you must use `4001`.

4. Run the following command to create a password for the new administrative user and then enter the password:

   ```
   passwd <admin_name>
   ```

   In this command, `<admin_name>` is the administrative user name. For example:

   ```
   passwd aadsadmin
   ```

5. Run the following command to provide sudo privileges for the new administrative user:

   ```
   usermod -aG wheel <admin_name>
   ```

   For example:

   ```
   usermod -aG wheel aadsadmin
   ```

## RHEL packages management

The system layer requires additional RHEL packages, which are not available by default. To obtain these packages, you can do one of the following:

- Subscribe to the Red Hat subscription.

  Avaya recommends this option. For more information about the subscription process, see the Red Hat website https://www.redhat.com.

  **Important:**

  - If you use the Red Hat Network subscription, you must enable additional RPMs from the RHEL CLI as described in Installing optional RHEL RPMs on page 79.
  - For AWS software-only deployments, if you use the Red Hat Network subscription, you must assign a public IP address to each of your AWS instances using the AWS Elastic IP service.

- Create a local repository for RPM installation or updates.

### Installing optional RHEL RPMs

#### About this task

If you subscribe to the Red Hat subscription, you must enable the following RHEL repositories before installing the system layer:

- rhel-7-server-rpms
- rhel-7-server-optional-rpms

These repositories contain RPMs that are required for system layer installation.

#### Before you begin

Subscribe to the Red Hat subscription.

#### Procedure

1. Log in to the RHEL virtual machine as the root user using an SSH connection.
2. Run the following command to view the enabled repositories:

   ```
   yum repolist
   ```

3. Ensure that the command output contains the following entries in the “repo id”column:
   - `rhel-7-server-rpms/x86-64` for rhel-7-server-rpms.
   - `rhel-7-server-optional-rpms/x68_64` for rhel-7-server-optional-rpms
4. If the command output does not contain the required entries, do the following:
   - To enable the rhel-7-server-rpms repository, run the following command:

     ```
     subscription-manager repos --enable=rhel-7-server-rpms
     ```

   - To enable the rhel-7-server-optional-rpms repository, run the following command:

     ```
     subscription-manager repos --enable=rhel-7-server-optional-rpms
     ```

# Enabling FIPS for software-only systems

## About this task

FIPS is a cryptographic security standard. Use this procedure if your enterprise requires FIPS-compliant cryptographic algorithms only.

For software-only installations, FIPS mode is enabled at the operating system level before installing the system layer. If FIPS is enabled in the operating system, then Avaya Aura® Web Gateway is installed in FIPS mode. Otherwise, Avaya Aura® Web Gateway is installed in non-FIPS mode. FIPS installation is only supported for new installations. You cannot upgrade a non-FIPS system to a FIPS system. If you want to enable FIPS on a non-FIPS system or disable FIPS on a FIPS system, you must uninstall the Avaya Aura® Web Gateway application first, change FIPS mode, and then re-install Avaya Aura® Web Gateway.

**Important:**

- You must enable FIPS before installing the system layer.
- The following features are unavailable in FIPS mode:
  - OAuth / SAML authorization
  - Onboard Open LDAP

**Note:**

- If FIPS mode is enabled, you must use the Secure LDAP (LDAPS) protocol to configure LDAP.
- In cluster deployments, if FIPS mode is enabled, SSL encryption for internode communication between the database servers on the Avaya Aura® Web Gateway nodes is enabled by default.

## Procedure

1. Log in to the virtual machine as an administrator using an SSH connection.
2. Open the `/etc/ssh/sshd_config` file in a text editor with sudo privileges.

   For example, to open the file in vi, run the `sudo vi /etc/ssh/sshd_config` command.
3. Add the following three entries to the file:

   ```
   Ciphers aes256-ctr,aes192-ctr,aes128-ctr
   MACs hmac-sha2-512,hmac-sha2-256,hmac-sha1
   Kexalgorithms ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha1
   ```
4. Save the `/etc/ssh/sshd_config` file.
5. Open the `/etc/ssh/ssh_config` file in a text editor with sudo privileges.

   For example, to open the file in vi, run the `sudo vi /etc/ssh/ssh_config` command.

6. Add the following two entries to the file:

```
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
MACs hmac-sha2-512,hmac-sha2-256
```

7. Save the `/etc/ssh/sshd_config` file.
8. Complete the steps listed in the Federal standards and regulations section of the Red Hat documentation.

### Next steps

- Install the packages listed in Additional packages required for FIPS mode on page 81.
- Ensure that the Haveged service is running on the virtual machine. For more information, see Enabling the Haveged service on page 82.

**Related links**

Enabling FIPS mode on page 94

## Additional packages required for FIPS mode

If you want to use Avaya Aura® Web Gateway in FIPS mode, you must install the following packages:

- `haveged-1.9.1-1.el7.x86_64.rpm` or later.
- `tomcat-native-1.2.17-1.el7.x86_64.rpm` or later.

These packages are available from the Extra Packages for Enterprise Linux (EPEL) Fedora Special Interest Group.

For information about installing packages from the EPEL respistory see the EPEL FAQ. You must only install these packages if you deploy Avaya Aura® Web Gateway as a software-only application.

## Installing packages required for FIPS mode manually

### About this task

If you do not have the EPEL repository on your RHEL 7.6, you can install the packages required to enable FIPS mode manually.

### Before you begin

Download the following packages on your local machine:

- `haveged-1.9.1-1.el7.x86_64.rpm` or later
- `tomcat-native-1.2.17-1.el7.x86_64.rpm` or later

### Procedure

1. Log in to the virtual machine as the root user using an SSH connection.
2. Upload the packages to the virtual machine to the `/root` directory.

   Use a file transfer program of your choice, such as SFTP, SCP, or WinSCP.
3. Run the following commands:

```
rpm -ivh /root/<HAVEGED_PACKAGE_NAME>
rpm -ivh /root/<TOMCAT-NATIVE_PACKAGE_NAME>
```

For example:

```
rpm -ivh /root/haveged-1.9.1-1.el7.x86_64.rpm
```

### Enabling the Haveged service

#### About this task

Haveged is a random number generator based on the HAVEGE algorithm designed for the use on Linux systems. If you plan to use Avaya Aura® Web Gateway in FIPS mode, you must enable the Haveged service.

This procedure applies to software-only deployments and is not required for OVA-based deployments.

#### Before you begin

Install the Haveged package.

#### Procedure

1. Log in to the virtual machine as an administrator using an SSH connection.
2. Run the following command to start the Havaged service:

   ```
   systemctl start haveged
   ```

3. Run the following command to start Havged automatically after each system restart:

   ```
   systemctl enable haveged
   ```

## Installing the system layer

#### About this task

The system layer is low-level software that provides the required operational environment for the Avaya Aura® Web Gateway application.

During the installation process, the system downloads the required packages from the remote repository. The package installation might take up to 10 minutes depending on your network bandwidth.

#### Before you begin

- Install RHEL 7.6 on virtual machines.
- Create disk partitioning as described in Creating disk partitioning for software-only deployments on page 76.
- Enable the YUM package management on RHEL. For more information, see the Red Hat documentation on the https://www.redhat.com website.
- Create at least one non-root administrative user as described in Creating administrative users on page 78.
- Download the `csa-swonly-<AAWG_VERSION>.tgz` software-only installation package from PLDS.
- Obtain the FQDN of the IP address of a Network Time Protocol (NTP) server.

**Note:**

Avaya recommends using the NTP servers of your organization instead of public NTP servers.

- If you are planning to use FIPS, enable it as described in Enabling FIPS for software-only systems on page 80. You cannot enable FIPS mode during or after Avaya Aura® Web Gateway installation.

## Procedure

1. Upload the software-only installation package on the virtual machine to the `/root` directory.

   Use a file transfer program of your choice, such as SFTP, SCP or WinSCP.

2. Log in to the virtual machine as the root user.
3. To extract the content of the installation package, run the following command:

   `tar -xzf csa-swonly-<AAWG_VERSION>.tgz`

   For example: `tar -xzf csa-swonly-3.9.0.0.x.tgz`

   The `/root/csa-swonly-AAWG_RELEASE/` directory contains the following files:

   - The system layer package in TGZ archive `ucapp-swonly-system-<VERSION>.tgz`.
   - The Avaya Aura® Web Gateway application binary `csa-<AAWG_RELEASE>.bin`.

4. Go to the directory with the extracted installation package:

   `cd csa-swonly-<AAWG_VERSION>`

5. To extract the content of the archive with the system layer installation files, run the following command:

   `tar -xzf ucapp-swonly-system-<SYSTEM_LAYER_VERSION>.tgz`

   For example: `tar - xzf ucapp-swonly-system-1.0.0.0.1.tgz`

6. Go to the directory with the extracted system layer package:

   `cd ucapp-swonly-system-<SYSTEM_LAYER_VERSION>`

7. Run the following command to install the system layer:

   `./swOnlyUpdate.sh --install`

8. When the system prompts you to enable the Enhanced Access Security Gateway (EASG) functionality, do one of the following:

   - Enter `yes` to enable EASG.

     The EASG functionality enables Avaya support personnel to access your Avaya Aura® Web Gateway system and resolve product issues in real time. Avaya recommends enabling EASG during installation.
   - Enter `no` if you do not want to enable the EASG functionality.

   If you select `no`, you can enable it later if required.

9. When the system prompts you, provide the IP address or FQDN of the NTP server.
10. After the system reboots, run one of the following commands to ensure that system layer is installed:
    - `sys versions`
    - `/root/csa-swonly-<AAWG_RELEASE>/ucapp-swonly-system-<SYSTEM_LAYER_VERSION>/swOnlyUpdate.sh --status`

### Next steps

- Ensure that:
  - The NTP service is running.
  - System Manager and Session Manager are reachable.
- Install the Avaya Aura® Web Gateway application.

## Checking the NTP service status

### About this task

For the optimal functioning of the Avaya Aura® Web Gateway server, the local system clock must have an accuracy of 100 milliseconds or less. You must ensure that the NTP service is running on the virtual machine before installing the Avaya Aura® Web Gateway application.

### Procedure

1. Log in to the virtual machine CLI as the root user using an SSH connection.
2. Run the following command to verify that the NTP service is running:

   ```
   systemctl status ntpd
   ```

   Ensure that the system displays `active (running)`.
3. If the NTP service is not running, run the following command:

   ```
   systemctl start ntpd
   ```
4. Run the following command to verify that the system clock is synchronized:

   ```
   ntpstat
   ```
5. Ensure that the system displays `synchronized to NTP server`.
6. If the system clock is not synchronized, do the following:
   a. Run the following commands:

      ```
      systemctl stop ntpd
      ntpd -gq
      systemctl start ntpd
      ```
   b. Run the `ntpstat` command again to verify that the system clock is synchronized.

## Checking the connection to System Manager

### About this task

You must ensure that System Manager is reachable before installing the Avaya Aura® Web Gateway application.

### Procedure

1. Log in to the virtual machine CLI as an administrator using an SSH connection.
2. Run the following command:

   ```
   ping -c 10 <SMGR_ADDRESS>
   ```

   In this command, `<SMGR_ADDRESS>` is the FQDN of System Manager.

   If System Manager is reachable, the system displays the following output for the command:

   ```
   10 packets transmitted, 10 received, 0% packet loss
   ```

# Software-only deployment on Amazon Web Services

## Software-only installation checklist for Amazon Web Services

The following checklist outlines the tasks that you must perform when deploying Avaya Aura® Web Gateway as a software-only application in an AWS environment.

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 1 | Ensure that the virtual machines that you plan to use to deploy Avaya Aura® Web Gateway comply with the requirements for software-only installation. | Avaya Aura® Web Gateway supports c4.xlarge and c4.2xlarge AWS instance types. For more information, see Resources profile specifications for Avaya Aura Web Gateway on Amazon Web Services on page 31. | |
| 2 | Prepare your AWS instance for software-only installation. | See Prerequisites for software-only deployment on AWS on page 87. | |
| 3 | Download the Avaya Aura® Web Gateway software-only installation package from PLDS. | The software-only installation package includes the following files:<br>• Software-only system layer installer.<br>• Avaya Aura® Web Gateway application installer.<br>The package file name has the `csa-swonly-<AAWG_VERSION>.tgz` format. | |
| 4 | Create security groups on AWS. | See Creating security groups on page 87. | |
| 5 | Install Red Hat Enterprise Linux (RHEL) 7.6 on AWS. | Avaya Aura® Web Gateway Release 3.9 requires RHEL 7.6. For more information about installation, see Installing Red Hat Enterprise Linux 7.6 on AWS on page 89. | |

*Table continues…*

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 6 | Create disk partitioning on RHEL. | Avaya Aura® Web Gateway requires specific disk partitioning to organize data storage. For more information about creating disk partitioning, see Creating disk partitioning for software-only deployments on page 76 and Disk partitions for software-only deployments on page 76. | |
| 7 | Enable root access to RHEL. | RHEL deployed on AWS does not have the root user enabled by default. For more information, see Enabling root access on page 91. | |
| 8 | Create a non-root Linux user. | The installation and administration of the Avaya Aura® Web Gateway server is more secure when performed by non-root users with sudo privileges. For more information, see Creating administrative users on page 78. | |
| 9 | Enable the YUM package manager on RHEL. | The YUM package manager is used to install the required packages. For more information about enabling YUM, see the Red Hat YUM documentation. | |
| 10 | Enable FIPS mode (optional). | For software-only deployments, you can only enable FIPS mode before installing the system layer. For more information, see Enabling FIPS for software-only systems on page 80, Additional packages required for FIPS mode on page 81, and Enabling the Haveged service on page 82. | |
| 11 | Do one of the following to manage additional RHEL packages:<br>• Register your RHEL instance to the Red Hat subscription.<br>• Create a local repository for RPM installation or updates. | For more information, see RHEL packages management on page 79.<br>Registering your RHEL instance to the Red Hat subscription is the preferred option. | |
| 12 | Prepare you RHEL system for installing the software-only system layer. | See Prerequisites for installing the system layer on AWS on page 91. | |
| 13 | Install the software-only system layer on your RHEL. | The system layer is low-level software that forms the required operational environment for Avaya Aura® Web Gateway.<br>For more information, see Installing the system layer on page 82. | |

*Table continues…*

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 14 | In cluster deployments, create target groups for the load balancer. | See Creating target groups on page 92. | |
| 15 | In cluster deployments, configure Elastic load balancers. | See Creating and configuring Elastic load balancers on page 93. | |
| 16 | Ensure that:<br>• The NTP service is up and running.<br>• System Manager is reachable from your virtual machine. | Perform these checks to ensure that the system layer is installed successfully so you can install the Avaya Aura® Web Gateway application.<br>For more information, see Checking the NTP service status on page 84 and Checking the connection to System Manager on page 84. | |

## Prerequisites for software-only deployment on AWS

- Use standard Amazon Web Services procedures to create the required network setup, including Virtual Private Cloud and subnet settings.
- Add records with the Avaya Aura® Web Gateway front-end FQDN to your DNS or AWS Route 53 hosted zone.
- Ensure that you have an NTP server. You can deploy your own NTP server or use the NTP server provided by AWS.
- Create key pairs. For more information, see Creating a key pair on page 58.
- If you are deploying an Avaya Aura® Web Gateway cluster, create load balancer certificates for the Avaya Aura® Web Gateway virtual FQDN.

  For more information, see Creating and applying load balancer certificates on page 65.

## Creating security groups

### About this task

AWS uses security groups to control inbound and outbound traffic. For software-only installation, you must create the following security groups:

- Avaya Aura® Web Gateway security group.

  This security group uses the primary eth0 interface.
- Avaya Aura® Web Gateway load balance security group.

### Procedure

1. On the Amazon Web Services Management console, navigate to **Services** > **EC2** > **Security group**.
2. Click **Create Security Group**.
3. In **Security group name**, type a name of your choice.

   For example: `AAWG security group eth0`

4. **(Optional)** In **Description**, type a description for the group.
5. From **VPC**, select the Virtual Private Cloud that you plan to use for Avaya Aura® Web Gateway.
6. Configure the inbound and outbound traffic rules for the group.

   Fore more information, see the “Traffic rules” section for the appropriate group.
7. Repeat steps 2 on page 87 to 6 on page 88 to create the additional required security groups.

## Traffic rules for the Avaya Aura® Web Gateway security group

### Inbound rules

| Type | Protocol | Port range | Source |
|---|---|---|---|
| Custom TCP | TCP | 31415 | 0.0.0.0/0 |
| Custom TCP | TCP | 8447 | 0.0.0.0/0 |
| Custom TCP | TCP | 7001 | 0.0.0.0/0 |
| Custom TCP | TCP | 8468 | 0.0.0.0/0 |
| Custom TCP | TCP | 8543 | 0.0.0.0/0 |
| Custom TCP | TCP | 7000 | 0.0.0.0/0 |
| HTTPS | TCP | 443 | 0.0.0.0/0 |
| Custom TCP | TCP | 8457 | 0.0.0.0/0 |
| Custom TCP | TCP | 3268 | 0.0.0.0/0 |
| Custom TCP | TCP | 8448 | 0.0.0.0/0 |
| Custom TCP | TCP | 21000 | 0.0.0.0/0 |
| Custom TCP | TCP | 9999 | 0.0.0.0/0 |
| SSH | TCP | 22 | 0.0.0.0/0 |
| Custom TCP | TCP | 8440 | 0.0.0.0/0 |
| Custom TCP | TCP | 2009 | 0.0.0.0/0 |
| Custom TCP | TCP | 8458 | 0.0.0.0/0 |
| Custom TCP | TCP | 3269 | 0.0.0.0/0 |
| Custom TCP | TCP | 8445 | 0.0.0.0/0 |
| Custom TCP | TCP | 161 | 0.0.0.0/0 |
| Custom TCP | TCP | 8442 | 0.0.0.0/0 |

### Outbound rules

| Type | Protocol | Port range | Source |
|---|---|---|---|
| All traffic | All | All | 0.0.0.0/0 |
| All traffic | All | All | ::/0 |

### Traffic rules for the Avaya Aura® Web Gateway load balancer security group

#### Inbound rules

| Type | Protocol | Port range | Source |
|---|---|---|---|
| Custom TCP | TCP | 8440 | 0.0.0.0/0 |
| Custom TCP | TCP | 8443 | 0.0.0.0/0 |
| HTTPS | TCP | 443 | 0.0.0.0/0 |
| Custom TCP | TCP | 8445 | 0.0.0.0/0 |

#### Outbound rules

| Type | Protocol | Port range | Source |
|---|---|---|---|
| All traffic | All | All | 0.0.0.0/0 |
| All traffic | All | All | ::/0 |

## Installing Red Hat Enterprise Linux 7.6 on AWS

### About this task

Use this procedure to deploy the RHEL 7.6 operating system on your AWS instance. If you are deploying a cluster, repeat this procedure for each Avaya Aura® Web Gateway node.

### Before you begin

Create security groups.

### Procedure

1. On the Amazon Web Services Management console, navigate to **Services** > **EC2** .
2. Click **Launch instance**.
3. On the Choose an Amazon Machine Image page, in the left pane, click **Community AMIs** and then click the **Red Hat** check box.
4. From the list of operating systems, select the **RHEL 7.6** and then click **Select**.

   The following is an example of the RHEL 7.6 name: **RHEL-7.6_HVM-GA-20181017-X86_64-0-hOURLY2-gp2**
5. On the Choose an Instance Type page, select either the **c4.xlarge** or **c4.2xlarge** type depending on your deployment and then click **Next**.
6. On the Configure Instance Details page, configure the settings as follows:
   a. In **Network**, select the VPC that you configured for your deployment.
   b. In **Subnet**, select the subnet that you configured for your deployment.
   c. In **Domain join directory**, select one of the following:
      - If you plan to use your own DNS server, select **No directory**.
      - If you plan to use the AWS Route 53 for DNS, select an appropriate domain from Route 53.

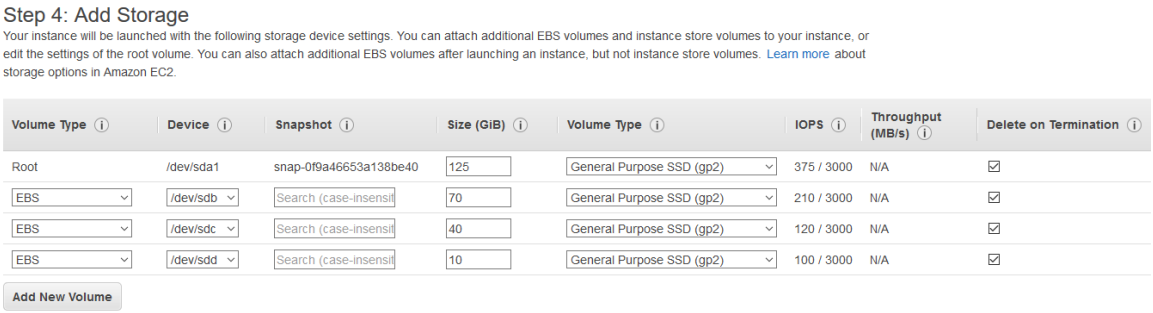
d. In the Network interfaces area, create the ethernet network interface with the `eth0` name and the IP address of the Avaya Aura® Web Gateway node.

e. For other parameters, keep the default values.

7. On the Add Storage page, create four EBS volumes using the values provided in Disk partitions for software-only deployments on page 76.

   For **Volume type**, use **General Purpose SSD (gp2)** for all volumes.

   The following image shows the configured volumes:




8. **(Optional)** On the Add Tags page, add tags for the management instance and volumes.
9. On the Configure Security Group page, do the following:

   a. In **Assign a security group**, select **Select an existing security group**.

   b. Select the Avaya Aura® Web Gateway security group that you created when configuring security groups.

10. On the Review Instance Launch page, verify the instance settings and then click **Launch**.

### Next steps

If you are using your own DNS server or a public DNS server, configure DNS settings as described in Configuring DNS settings on RHEL on page 90.

## Configuring DNS settings on RHEL

### About this task

If do not use the Route 53 DNS service, you must provide the IP address of a DNS server that you plan to use on RHEL.

### Before you begin

Install RHEL on AWS.

### Procedure

1. Log in to the RHEL as the root user using an SSH connection.
2. Open the `/etc/resolv.conf` file in a text editor.

   For example: `vi /etc/resolv.conf`

3. Add the following entry to the file:

```
nameserver <DNS_ADDRESS>
```

In this entry, `<DNS_ADDRESS>` is the IP address of the DNS server that you plan to use in your deployment.

4. **(Optional)** Do one of the following:
   - If the file does not contain the `search` entry, add the following entry:

     ```
     search <DOMAIN_NAME>
     ```

     In this entry, `<DOMAIN_NAME>` is your domain name. For example: `search mycompany.com`
   - If the file contains the `search` entry, enter your domain name at the end of the entry.

     Domain names must be separated with space characters. For example: `search example.com mydomain.com`
5. Save the file.

## Enabling root access

### About this task

You must use the root user to install the system layer. On RHEL installed on AWS, the root user is disabled by default, therefore you must enable it.

### Procedure

1. Log in to your AWS instance using the AWS CLI as the ec2-user.

   This is the default administration user, which does not require a login password.
2. Run the following command to edit the `/etc/ssh/sshd_config` file:

   ```
   sudo vi /etc/ssh/sshd_config
   ```
3. Add the following line to the file:

   ```
   PermitRootLogin yes
   ```
4. Save the file.
5. Run the following command to apply the changes:

   ```
   sudo service sshd restart
   ```
6. Set a password for the root user using the following command:

   ```
   sudo password root
   ```

## Prerequisites for installing the system layer on AWS

In addition to the prerequisites for the software-only system layer installation that are common for all deployment types, AWS has the following specific prerequisites:

- Ensure that you configured the Avaya Aura® Web Gateway front-end FQDN in the AWS Route 53 service or the DNS service that you use.

- On all Avaya Aura® Web Gateway nodes in your deployment, add information about each Avaya Aura® Web Gateway node to the `/etc/hosts` file in the following format:

  *<IP_Address> <Corresponding_FQDN> <hostname>*

  For example:

  ```
  195.51.100.5 aawg1.mycompany.com aawg1
  195.51.100.6 aawg2.mycompany.com aawg2
  ```

- Enable root access to RHEL. For more information, see Enabling root access on page 91.
- Create a non-root user on RHEL. For more information, see Creating administrative users on page 78.
- If you are using a Red Hat subscription for RHEL package management, you must configure a public IP address on each of your AWS instances using the AWS Elastic IP service. For more information about setting up public IP addresses, see Elastic IP addresses.
- RHEL 7.6 released on AWS does not have LVM by default. You must install the LVM package manually by running the following command:

  ```
  yum install -y lvm2
  ```

## Creating target groups

### About this task

In cluster deployments, target groups forward traffic from the load balancer to a specific node of the Avaya Aura® Web Gateway cluster when certain conditions are met.

You must configure two target groups for Avaya Aura® Web Gateway node IP addresses with the following parameters:

| Group | Protocol | Port | IP to register |
|---|---|---|---|
| Target group for Avaya Aura® Web Gateway nodes #1 | HTTPS | 8448 | IP addresses of all Avaya Aura® Web Gateway nodes in the cluster.<br>These are the IP addresses of the primary eth0 interface of cluster nodes. |
| Target group for Avaya Aura® Web Gateway nodes #2 | HTTPS | 8445 | IP addresses of all Avaya Aura® Web Gateway nodes in the cluster.<br>These are the IP addresses of the primary eth0 interface of cluster nodes. |

Only perform this procedure if you have an Avaya Aura® Web Gateway cluster.

### Procedure

Repeat the following steps for each target group:

1. On the Amazon Web Services Management console, navigate to **Services** > **EC2** > **Target Groups**.
2. Click **Create target group**.

   The Amazon Web Services Management displays the Specify group details page.

3. In the Basic configuration area, configure settings as follows:
    a. In **Choose a target type**, select **IP addresses**.
    b. In **Target group name**, type a name of your choice for the group.
    c. In **Protocol**, select the protocol specified for the group in the “Protocol” column of the table.
    d. In **Port**, type the port number specified for the group in the “Port” column of the table.
    e. In **VPC**, select the Virtual Private Cloud that you are using for your deployment.
    f. In **Protocol version**, select **HTTP1**.
4. In the Health checks area, configure the settings as follows:
    a. In **Health check protocol**, select **HTTP**.
    b. In **Health check path**, type `/health`.
5. Click **Next**.
6. On the Register targets page, configure IP addresses for the group as follows:
    a. In **IP**, type the IP address of a node as specified in the “IP to register” column of the table for the group you are configuring.
    b. In **Port**, type the port number specified for the group in the “Port” column of the table.
    c. Click **Include as pending below**.
    d. Repeat substeps a to c for all remaining IP addresses that you must include in the group.
7. Click **Create target group**.

## Creating and configuring Elastic load balancers

### About this task

The Elastic load balancer distributes incoming traffic between Avaya Aura® Web Gateway nodes. In cluster deployments, you must create one Elastic load balancer for Avaya Aura® Web Gateway nodes.

### Before you begin

- Create two target groups as described in Creating target groups on page 92.
- Ensure that you have the load balancer certificates for the Avaya Aura® Web Gateway front-end FQDN. For more information about creating certificates, see Creating and applying load balancer certificates on page 65.

### Procedure

1. On the Amazon Web Services Management console, navigate to **Services** > **EC2** > **Load Balancers**.
2. Click **Create Load Balancer**.

3. On the Configure Load Balancer page, configure the settings as follows:
   a. In **Name**, type a name of your choice.
   b. In **Scheme**, select **Internal**.
   c. In **IP address type**, select **ipv4**.
   d. In **VPC**, select the Virtual Private Cloud that you are using for your deployment.
   e. In **Listener**, add listeners for the load balancer as follows:

| Load balancer | Protocol | Port |
|---|---|---|
| Avaya Aura® Web Gateway load balancer | HTTPS | 443 |
| | HTTPS | 8440 |
| | HTTPS | 8443 |
| | HTTPS | 8445 |

   f. In **Availability Zones**, select the subnet that you configured for all nodes in the cluster.
4. On the Configure Security Settings page, in **Certificate Type**, select **Choose a certificate from ACM** and then select the certificates that you prepared for the Avaya Aura® Web Gateway FQDN.
5. On the Configure Security Groups page, in **Assign a security group**, select **Select an existing security group** and then select the Avaya Aura® Web Gateway load balancer security group that you created.

   For more information about security groups, see Creating security groups on page 87.
6. On the Configure Routing page, configure routing as follows:
   a. In **Target**, select **Existing target group**.
   b. In **Name**, select the target groups related to Avaya Aura® Web Gateway nodes.

      For more information about the target groups, see Creating target groups on page 92.
7. On the **Register Targets** page, click **Next: Review**.
8. Click **Create**.

# Enabling FIPS mode

## About this task

FIPS is a cryptographic security standard. Use this procedure if your enterprise requires FIPS compliance.

FIPS mode is enabled at the operating system level before starting the Avaya Aura® Web Gateway installation. If FIPS is enabled for the operating system, then Avaya Aura® Web Gateway will be installed in FIPS mode. Otherwise, Avaya Aura® Web Gateway will be installed in non-FIPS mode. FIPS installation is only supported for new installations. You cannot upgrade a non-FIPS

system to a FIPS system. If you want to enable FIPS on a non-FIPS system or disable FIPS on a FIPS system, you must uninstall the Avaya Aura® Web Gateway application first, change FIPS mode, and then install Avaya Aura® Web Gateway.

**Note:**

- This procedure applies to OVA-based deployments. If you deploy Avaya Aura® Web Gateway as a software-only application, you must enable FIPS mode using the procedure for software-only deployments.
- If FIPS mode is enabled, you must use the Secure LDAP (LDAPS) protocol to configure LDAP.
- In cluster deployments, if FIPS mode is enabled, SSL encryption for internode communication between the database servers on the Avaya Aura® Web Gateway nodes is enabled by default.
- OAuth authorization is unavailable in FIPS mode.

### Procedure

1. Log in to the virtual machine with the Avaya Aura® Web Gateway OVA as an administrator.
2. Run the following command to enable FIPS mode:

   ```
   sys secconfig --fips --enable
   ```

3. **(Optional)** To review the FIPS status, run the following command:

   ```
   sys secconfig --fips --query
   ```

### Related links

Enabling FIPS for software-only systems on page 80

# Disabling FIPS mode

### About this task

After Avaya Aura® Web Gateway is installed with FIPS mode enabled, you *cannot* switch back to non-FIPS mode. You must uninstall the Avaya Aura® Web Gateway application layer first, disable FIPS mode, and then reinstall Avaya Aura® Web Gateway.

### Procedure

1. Uninstall Avaya Aura® Web Gateway.

   For more information, see Uninstalling the Avaya Aura Web Gateway on page 97.

2. Run the following command:

   ```
   sys secconfig --fips --disable
   ```

# Enabling additional STIG hardening

## About this task

The Security Technical Implementation Guides (STIGs) are the requirements that, when implemented, enhance application security and monitoring capabilities. By default, Avaya Aura® Web Gateway enables essential STIG hardening options during the system layer installation or upgrade. These default settings are appropriate for most deployments. If your organization requires stricter STIG compliance, use this procedure to enable additional Linux STIG security hardening options.

**Important:**

You *cannot* enable additional STIG hardening in software-only deployments.

## Procedure

1. Log in to the virtual machine with the Avaya Aura® Web Gateway OVA as an administrator.
2. Run the following command to enable additional STIG hardening options:

   ```
   sys secconfig --stig --enable
   ```

3. When prompted, press `C` to apply new password rules.
4. **(Optional)** To review the STIG hardening status, run the following command:

   ```
   sys secconfig --stig --query
   ```

# Disabling additional STIG hardening

## About this task

Use this procedure to disable additional STIG hardening. The default STIG hardening options, which are enabled during the system layer installation or upgrade process, will still be available. Avaya Aura® Web Gateway also continues to use the password complexity rules that were set up when you enabled additional STIG hardening.

## Procedure

1. Log in to the virtual machine with the Avaya Aura® Web Gateway OVA as an administrator.
2. Run the following command to disable additional STIG hardening:

   ```
   sys secconfig --stig --disable
   ```

3. **(Optional)** To review the STIG hardening status, run the following command:

   ```
   sys secconfig --stig --query
   ```

# Uninstalling the Avaya Aura® Web Gateway

### Procedure

1. Open the Linux shell using your Linux administrator account credentials.
2. To remove the Avaya Aura® Web Gateway from the system, run the following command:

   ```
   app uninstall
   ```

3. When prompted, type the following:
   a. **`uninstall`** and press `Enter`.
   b. **`yes`** and press `Enter`.

# Chapter 6: Avaya Aura® Web Gateway setup

## Installing the Avaya Aura® Web Gateway

### About this task

Use this procedure to install a standalone Avaya Aura® Web Gateway or the initial node for an Avaya Aura® Web Gateway cluster.

**Important:**

Do not use this procedure to install additional nodes to a cluster. For more information on installing additional nodes, see Installing additional nodes to create a cluster on page 104.

### Before you begin

- Deploy the Avaya Aura® Web Gateway OVA.
- Start the virtual machine.
- If you are planning to use FIPS, enable it as described in Enabling FIPS mode on page 94. You *cannot* enable FIPS mode during or after Avaya Aura® Web Gateway installation. You cannot use the OAuth authentication feature when FIPS mode is enabled.

### Procedure

1. Open the Linux shell using your Linux administrator account credentials.

   The Linux administrator account is created during the deployment process.

2. Do one of the following:

   - If you install Avaya Aura® Web Gateway using the OVA, run the following command:

     ```
     app install
     ```

     When you run the `app install` command without specifying a build, then the system automatically picks up the current build in `opt/Avaya`. If you do specify a build by running `app install csa-<version>.bin`, then the system looks for that build first in your current working directory and then in `opt/Avaya`.

   - If you install Avaya Aura® Web Gateway as a software-only application, run the following command:

     ```
     app install <PATH>/<INSTALLER>
     ```

In this command, `<PATH>` is the full path to the directory where you extracted the application binary when installing the system layer, and `<INSTALLER>` is the Avaya Aura® Web Gateway application binary. For example:

```
app install /root/csa-swonly-3.9.0.0/csa-3.9.0.0.bin
```

The system displays the installation screen.

**Important:**

During the installation, do not resize the screen or the SSH console.

3. If you are installing the initial node for a new cluster, then do the following:
   a. Select **Cluster Configuration**.
   b. Ensure that **Initial cluster node** is set to `y` (yes) and **Local Node IP address** is set to the IP address of the node.

      These are the default values.

      To return to the previous menu, select **Return to Main Menu** and press `Enter`.
   c. **(Optional)** In the **Cassandra Encryption** menu, enable SSL encryption to secure Cassandra database communications between nodes in a cluster.

      **Important:**

      - If you want to enable Cassandra internode encryption, you must enable it during the initial installation. This setting cannot be changed after the initial installation.
      - If you enabled FIPS mode, ensure that Cassandra internode encryption remains enabled. If you disable Cassandra internode encryption, installation will fail.
4. Select **Front-end host, System Manager and Certificate Configuration** and do the following:
   a. For a standalone node, select **Front-end IP or FQDN** and enter the FQDN that clients use to access services.

      The default value is the FQDN assigned to the local server.

      For a cluster deployment that uses the internal load balancer, you must configure **Front-end IP or FQDN** as the FQDN corresponding to the virtual IP address of the internal load balancer.

      For a cluster deployment that uses an external load balancer, you must configure **Front-end IP or FQDN** as the FQDN corresponding to the external load balancer.
   b. Select **System Manager FQDN** and enter the FQDN of the Avaya Aura® System Manager that signs the certificates for Avaya Aura® Web Gateway services.
   c. **(Optional)** Select **System Manager web admin username (o)** and **System Manager web admin password** and provide the credentials.

d. Select **System Manager HTTPS Port** and type the port for contacting the REST interface of Avaya Aura® System Manager.

   The default port is 443.

e. Select **System Manager Enrollment Password** and type the Avaya Aura® System Manager enrollment password.

f. Select **Keystore password** and type a password to use for the local keystore.

   **Important:**

   You must remember the Keystore password for future references. You need this password for any certificate management tasks.

g. Configure additional settings that are required for your system as described in Front-end host, System Manager, and certificate configuration on page 109.

   To return to the previous menu, select **Return to Main Menu** and press `Enter`.

5. Select **Deployment settings** and then press the `Spacebar` to select the deployment option that corresponds to the solution that you are installing.

   If you have conferencing in your solution, then select **Team Engagement + Conferencing**. Otherwise, you must select **Team Engagement**. Do not select **Conferencing only**.

6. To review the settings, select **Continue** and then select **Accept and continue**.

   The system runs pre-install configuration checks.

7. To install the software, select **Continue** and then accept the license agreement.

   Wait for several minutes while the installation proceeds.

8. Select **Continue** to start the configuration utility.

   **Important:**

   Do not change the settings in **Front-end host, System Manager and Certificate Configuration** without reentering the System Manager enrollment and keystore passwords before applying the changes.

9. Select **LDAP Configuration**, and then configure each of the LDAP settings using the LDAP configuration information for your network.

   For more information on LDAP configuration, see LDAP configuration on page 112.

10. **(Optional)** If this is an initial node for a cluster, and you want to use internal load balancing, do the following:

    **Important:**

    - The virtual IP address is used for redundancy management of the internal load balancer in a cluster.
    - To avoid performance degradation of the cluster, an external load balancer is recommended for clusters with four or more nodes.

- For a cluster deployment that uses an external load balancer, you must configure **Front-end IP or FQDN** as the FQDN corresponding to the external load balancer.
- If you use an external load balancer, do not configure the virtual IP settings that enable the internal load balancer.

a. Select **Clustering Configuration** > **Virtual IP Configuration**.
b. Select **Enable virtual IP** and set the value to `y` (yes).

   The system displays additional Virtual IP configuration.
c. Configure all of the Virtual IP settings as described in Virtual IP configuration options on page 128.

   You must configure the initial node as the Virtual IP master node. In a cluster, you must configure one additional node as the Virtual IP backup node.

   **Important:**

   You must save the Virtual IP authentication password. You need this password when configuring the second node in the cluster as the virtual IP backup node.
d. To save the changes on the system, select **Apply** and then select **Continue**.
e. Select **Return to Main Menu** and press `Enter`.

11. To apply the changes, from the main menu, select **Continue** and then select **Yes** to start the services.

    The system starts the services.
12. To exit the configuration tool, select **Continue**.

### Next steps

- Set up the required certificates as described in Certificate configuration using the configuration utility on page 188.
- Install additional nodes to create a cluster.
- Change the following default passwords:
  - The default Cassandra database password as described in Changing the Cassandra user name and password on page 130. If you install a cluster, install all required additional nodes before changing the password.
  - The default password for automatic backups. For more information, see Changing the default password for automatic backups on page 131.

# Unexpected characters in the /etc/hosts file on a localhost line

## Condition

When you deploy Avaya Aura® Web Gateway on AWS, Avaya Aura® Web Gateway displays the following error:

```
Hostname Check ..........................................
Found unexpected characters in /etc/hosts on a localhost line
```

```
(127.0.0.1 or localhost )
Hostname Check ..................................... [FAILED]
```

### Cause

The `/etc/hosts` file is incorrectly configured when the virtual machine is created.

The following is an example of incorrectly configured localhost entries in the `/etc/hosts` file:

```
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
```

### Solution

1. Open the `/etc/hosts` file in the vi text editor with sudo privileges:

   ```
   sudo vi /etc/hosts
   ```

2. Reconfigure the lines that contain localhost entries as shown in the following example:

   ```
   127.0.0.1 localhost.localdomain localhost
   ::1 localhost6.localdomain6 localhost6
   ```

   Ensure that the lines does not contain any redundant space and tab characters.

3. Save the `/etc/hosts` file.
4. Repeat the Avaya Aura® Web Gateway installation procedure.

# Performing a silent installation

### About this task

Use this procedure to perform a silent installation of the Avaya Aura® Web Gateway server.

The silent installation consists of configuring most of the settings in a properties file, instead of using the installation and the configuration menu for every item.

The properties file is called `installation.properties`. It contains the same settings that you configure during the interactive installation. The settings are grouped, and the file contains comments that describe the settings.

**Note:**

The properties file does not contain settings for the following elements:

- The Avaya Aura® Web Gateway cluster
- The SSH RSA configuration

You must configure these settings using the configuration utility after the silent installation is complete.

If errors occur after the installation, you can use the configuration utility to re-configure some of the settings.

### Procedure

1. From the Avaya Aura® Web Gateway binary file, extract the template file.

   ```
   sudo ./csa-<version>.bin --tar xf -- ./installation.properties
   ```

2. Configure the settings in the `installation.properties` file.

   The settings are the same as the interactive installation. For more information about the settings, see Avaya Aura Web Gateway initial configuration settings on page 108.

   You can leave some of the settings blank and then configure them manually after the installation is complete.

3. Run the Avaya Aura® Web Gateway binary with a parameter that represents the full path to the properties file.

   For example:

   ```
   sudo ./csa-<version>.bin /home/avaya/installation.properties
   ```

4. **(Optional)** To start the Avaya Aura® Web Gateway service, run the following command:

   ```
   svc csa start
   ```

5. Manually configure the remaining items.

   When possible, use the web administration portal to modify configuration settings instead of the configuration utility. For more information about using the web administration portal, see *Administering the Avaya Aura® Web Gateway*.

## Seed node replacement configuration

If a seed node is unavailable, you might experience service loss on an Avaya Aura® Web Gateway cluster. You will also be unavailable to install a new node on the cluster. To prevent this issue from occurring, you can specify a list of backup nodes for the seed node while performing silent installation. If the initial seed node becomes unavailable, Cassandra replaces it with a node from the backup nodes list, so the cluster continues to operate. When you add a new node, Cassandra checks whether the initial seed node is available. If not, Cassandra tries to connect the new node to one of backup nodes.

**Important:**

You cannot configure backup nodes using the standard, interactive installation process.

Specify backup nodes in the SEED_NODE_BACKUP property of the `installation.properties` file. The value of this parameter is a list of IP addresses separated by commas. For example: `SEED_NODE_BACKUP=192.168.150.3,192.168.150.4`. If the seed node is unavailable, Cassandra tries to replace it with a node listed in SEED_NODE_BACKUP in the order specified in the property. On Avaya Aura® Web Gateway, you can review the seed nodes configuration in the `/opt/Avaya/CallSignallingAgent/<version>/cassandra/<version>/conf/cassandra.yaml` file.

### Related links

Installing additional nodes to create a cluster on page 104

# Installing additional nodes to create a cluster

## About this task

You can achieve redundancy and increase capacity by creating a cluster of Avaya Aura® Web Gateway nodes.

The installation procedure for each additional node is similar to the procedure for a single-server or initial node installation, with the addition of some cluster specific configuration. After installing an initial node, use this procedure to create a cluster of Avaya Aura® Web Gateway nodes. You can also use this procedure to add nodes to an existing cluster at a later time.

The virtual IP address and the IP addresses for all nodes of the cluster must be in the same network.

**Important:**

- When creating or expanding a cluster, for each additional Avaya Aura® Web Gateway node you must use the same resource profile that you used for the initial node. Mixed resource profile clusters are not supported. The resource profiles are set when installing the Avaya Aura® Web Gateway OVA and cannot be modified after the OVA is deployed.
- To avoid performance degradation of the cluster, an external load balancer is recommended for clusters with four or more nodes.

## Before you begin

- Install an initial Avaya Aura® Web Gateway node. For more information, see Installing the Avaya Aura Web Gateway on page 98.
- Enable the virtual IP configuration on the initial node if you are using the internal load balancer for the cluster.
- Configure the front-end FQDN on the initial node to match the FQDN assigned to the load balancer. If you need to update the front-end FQDN on the initial node, use the configuration utility.
- Deploy an OVA on the same network as the initial node for each additional node required. For more information, see VMware deployments on page 51.
- If you are planning to use FIPS, enable it as described in Enabling FIPS mode on page 94. You *cannot* enable FIPS mode during or after Avaya Aura® Web Gateway installation. You cannot use the OAuth authentication feature when FIPS mode is enabled.

## Procedure

1. Open the Linux shell using your Linux administrator account credentials.

   The Linux administrator account is created during the deployment process.

2. Do one of the following:

   - If you install Avaya Aura® Web Gateway using the OVA, run the following command:

     ```
     app install
     ```

     When you run the `app install` command without specifying a build, then the system automatically picks up the current build in `opt/Avaya`. If you do specify a build by

running `app install csa-<version>.bin`, then the system looks for that build first in your current working directory and then in `opt/Avaya`.

- If you install Avaya Aura® Web Gateway as a software-only application, run the following command:

```
app install <PATH>/<INSTALLER>
```

In this command, `<PATH>` is the full path to the directory where you extracted the application binary when installing the system layer, and `<INSTALLER>` is the Avaya Aura® Web Gateway application binary. For example:

```
app install /root/csa-swonly-3.9.0.0/csa-3.9.0.0.bin
```

The system displays the installation screen.

**Important:**

During the installation, do not resize the screen or the SSH console.

3. Select **Cluster Configuration** and do the following:
   a. Set the **Initial cluster node** option to `n` (no).
   b. Ensure that **Local Node IP address** is set to the IP address of the current node.
   c. Set **Cluster seed node** to the IP address of the initial node.
   d. Set **User ID (UID) of product user on seed node** to the user ID of the Linux administrator that was used to install the initial Avaya Aura® Web Gateway node.

      The default value is 4000.

      To determine the required UID, open the Linux shell on the initial node using your administrator credentials and then run the following command:

      ```
      id -u <adminuser>
      ```

   e. To save the changes on the system, select **Apply** and then select **Continue**.
   f. Select **Return to Main Menu** and press `Enter`.
4. In the **Cassandra Encryption** menu, enable SSL encryption to secure Cassandra database communications between nodes in a cluster.

   **Important:**

   - If you want to enable Cassandra internode encryption, you must do so during the initial installation. This setting cannot be changed after the initial installation.
   - If you enabled FIPS mode, ensure that Cassandra internode encryption remains enabled. If you disable Cassandra internode encryption, installation will fail.
5. Select **Front-end host, System Manager and Certificate Configuration** and do the following:
   a. Select **System Manager FQDN** and enter the FQDN of the Avaya Aura® System Manager that signs the certificates for Avaya Aura® Web Gateway services.

b. **(Optional)** Select **System Manager web admin username (o)** and **System Manager web admin password** and provide the credentials.

c. Select **System Manager HTTPS Port** and type the port for contacting Avaya Aura® System Manager.

   The default port is 443.

d. Select **System Manager Enrollment Password** and type the Avaya Aura® System Manager enrollment password.

e. Select **Keystore password** and type a password for using the local keystore.

   The keystore password on additional nodes should match the keystore password for the initial node.

   **Important:**

   You must remember the keystore password for future reference. You need this password for other certificate management tasks.

f. Configure additional settings that are required for your system as described in Front-end host, System Manager, and certificate configuration on page 109.

   To return to the previous menu, select **Return to Main Menu** and press `Enter`.

6. Select **Deployment settings** and then press the `Spacebar` to select the deployment option that corresponds to the solution that you are installing.

   You must configure the same deployment type that you configured on the initial node.

   If you have conferencing in your solution, then select **Team Engagement + Conferencing**. Otherwise, you must select **Team Engagement**. Do not select **Conferencing only**.

7. To review the settings, select **Continue** and then select **Accept and continue**.

   The system runs pre-install configuration checks.

8. To install the software, select **Continue** and then accept the license agreement.

   Wait for several minutes while the installation proceeds.

9. Select **Continue** to start the configuration utility.

   **Important:**

   Do not change the settings in **Front-end host, System Manager and Certificate Configuration** without reentering the System Manager enrollment and keystore passwords before applying the changes.

   **Warning:**

   Do not configure the LDAP settings on nodes that you add to a cluster. The LDAP configuration is automatically configured for additional nodes when they connect to the initial node.

10. If this is the second node of a cluster and the virtual IP for internal load balancing is enabled on the initial node, then do the following:

**Important:**

The virtual IP must be enabled only for the initial node and the second node. Do not enable the virtual IP on any other nodes.

a. Select **Clustering Configuration** > **Virtual IP Configuration**.

b. Select **Enable virtual IP** and set the value to `y` (yes).

The system displays additional Virtual IP configuration.

c. Configure all of the Virtual IP settings as described in Virtual IP configuration options on page 128.

**Important:**

You must use the same Virtual IP authentication password that you set on the initial node of the cluster.

d. To save the changes on the system, select **Apply** and then select **Continue**.

e. Select **Return to Main Menu** and press `Enter`.

11. To apply the changes, from the main menu, select **Continue** and then select **Yes** to start the services.

The system starts the services.

12. To exit the configuration tool, select **Continue**.

### Next steps

- Set up the required certificates as described in Certificate configuration using the configuration utility on page 188.
- Repeat this procedure to add the required number of nodes to the cluster.
- After all of the required cluster nodes are installed, change the default Cassandra database password as described in Changing the Cassandra user name and password on page 130.
- After all of the required cluster nodes are installed or if new nodes are added to an existing cluster, you must configure the RSA public and private keys on the initial node.

### Related links

Seed node replacement configuration on page 103

# Configuring RSA public and private keys for SSH connections in a cluster

### About this task

After nodes are added to a cluster, you must configure the RSA public and private keys to enable internode SSH communications.

Use this procedure to configure the RSA public and private keys on the initial node for the entire cluster.

### Before you begin

Install all of the required nodes for the cluster.

### Procedure

1. Log in to the Linux shell on the initial Avaya Aura® Web Gateway node as an administrator.
2. Run the Avaya Aura® Web Gateway configuration utility using the `app configure` command.
3. Navigate to **Clustering Configuration** > **Cluster Utilities** > **Configure SSH RSA Public/ Private Keys**.

   Avaya Aura® Web Gateway displays the RSA Public and Private key configuration tool.
4. When the system displays the `Add additional hosts to the list? (y/n)` prompt, enter `y` (yes) if you are generating keys for the first time or if you need to generate keys for a new node in the cluster.

   Otherwise, enter `n` (no).
5. If you chose to update the node list in the previous step, when Avaya Aura® Web Gateway prompts you, enter the IP address of the non-seed node in the cluster you want to generate keys for and then press `Enter`.
6. Repeat the previous step for all remaining non-seed nodes.
7. When Avaya Aura® Web Gateway prompts you to enter a user name for a node, enter the username for the Linux administrator account that you used to perform the Avaya Aura® Web Gateway installation.
8. If Avaya Aura® Web Gateway prompts you to replace the existing keys, enter `y` (yes).
9. If Avaya Aura® Web Gateway displays the following error, type `yes` and then press `Enter`:

   ```
   The authenticity of the host can't be established.
   ```
10. When Avaya Aura® Web Gateway prompts you to enter a password, enter the password for the Linux administrator account that you used to perform the installation.
11. When the configuration is complete, press `Enter`.
12. Return to the main menu.
13. From the main menu, select **Continue** and then select **Yes** to restart services and apply the changes.

# Avaya Aura® Web Gateway initial configuration settings

The following sections describe the initial configuration settings for Avaya Aura® Web Gateway. They also list the equivalent `installation.properties` file parameters for each setting for silent installations. If you do not configure a setting during installation, you can configure it later. You can update many of these settings anytime using the Avaya Aura® Web Gateway

administration portal as described in the “Avaya Aura® Web Gateway management with the administration portal” chapter in *Administering the Avaya Aura® Web Gateway*.

**Related links**

[Front-end host, System Manager, and certificate configuration](#) on page 109
[LDAP configuration](#) on page 112
[Cluster configuration](#) on page 127
[Virtual IP configuration options](#) on page 128
[Advanced configuration](#) on page 129

# Front-end host, System Manager, and certificate configuration

If you do not select the **Front-end host, System Manager and Certificate Configuration** option during the installation, then the self-signed certificates are automatically generated. Self-signed certificates are also generated when:

- The **System Manager FQDN** option is not set.
- The **Use System Manager for certificates** option is set to `n` and certificates were not provided for one of the interfaces: REST, OAMP, SIP, or NODE.

You can modify certificate configuration settings from the administration portal anytime. This is useful if you do not complete the certificate configuration as part of the initial setup process or if you generate certificates at a later time.

For information about managing certificates through the Avaya Aura® Web Gateway administration portal, see the managing certificates section in *Administering the Avaya Aura® Web Gateway*.

**Caution:**

If the system is using System Manager for certificates, then changing the System Manager FQDN after installation will result in the regeneration of certificates. This might impact the client and backend server communication with the Avaya Aura® Web Gateway.

**Table 3: Front-end host, System Manager and Certificate Configuration settings**

| Item name | Description | Equivalent `installation.properties` file parameter |
|---|---|---|
| **Front-end FQDN** | The front-end FQDN is the address that end-user clients use to access the services provided by Avaya Aura® Web Gateway .<br><br>For a cluster deployment, you must configure the front-end FQDN as the FQDN of the virtual IP address. If an external load balancer is used, set this value to the FQDN of the load balancer. | `REST_FRONTEND_HOST` |

*Table continues…*

| Item name | Description | Equivalent `installation.properties` file parameter |
|---|---|---|
| | The default value depends on the configuration present in the `/etc/hosts` file of the server. | |
| **System Manager FQDN** | The FQDN of the Avaya Aura® System Manager that signs the certificates. | `SYSTEM_MGR_IP` |
| **System Manager web admin username (o)** | The System Manager web administration portal user name. | `SMGR_USER_NAME` |
| **System Manager web admin password** | The System Manager web administration portal password. | `SMGR_USER_PASSWORD` |
| **System Manager HTTPS Port** | The HTTPS port used for the Alarm Agent for the current Avaya Aura® Web Gateway server.<br>The default value for this setting is 443. | `SYSTEM_MGR_HTTPS_PORT` |
| **System Manager Enrollment Password** | The Avaya Aura® System Manager enrollment password.<br>**Note:**<br>To get the password, log in to System Manager and navigate to **Service** > **Security** > **Certificates** > **Enrollment Password**. | `SYSTEM_MGR_PW` |
| **Override port for remote access** | Specifies the port on the Avaya Aura® Web Gateway server. This port is used by a reverse proxy, such as Avaya SBCE, that fronts HTTP-based clients which are external to the enterprise.<br>The reverse proxy continues to receive requests from the external clients on port 443, and then forwards them to the Avaya Aura® Web Gateway on the reverse proxy port. Clients within the enterprise continue to access Avaya Aura® Web Gateway directly using port 443.<br>Select `y` (yes) to configure the port for the reverse proxy server or `n` (no) to keep the default configuration that remains disabled. | `OVERRIDE_FRONTEND_PORT`<br>For the **Front-end port for reverse proxy** setting, the equivalent parameter is `REST_FRONTEND_PORT`. |

*Table continues…*

| Item name | Description | Equivalent `installation.properties` file parameter |
|---|---|---|
| | **Important:**<br>If this setting is enabled, you cannot set the port to 443, but you can set it to 8444, which is the default setting, or to any other port.<br>If you select `y` (yes), the menu displays a new setting for the reverse proxy port: **Front-end port for reverse proxy**.<br>If you override the port for remote access, you must configure this port on the Avaya SBCE external interface for Avaya Aura® Web Gateway. For more information, see *Administering Avaya Session Border Controller for Enterprise*.<br>**Note:**<br>You can also set this port on the Avaya Aura® Web Gateway administration portal under **External Access** > **HTTP Reverse Proxy**. After selecting the **Front-end port for remote access** check box, you can modify the port value. | |
| **Use System Manager for certificates** | Specifies if the certificates are retrieved from Avaya Aura® System Manager or from imported files.<br>Select `y` (yes) to retrieve certificates from Avaya Aura® System Manager or `n` (no) to retrieve certificates from imported files.<br>If you select `n` (no), the menu displays new settings for configuring the certificate files. To configure the certificate settings, you must provide the complete file path name to the: | `USE_SMGR`<br>If the `USE_SMGR` option is set to `n` (no), you must configure the following parameters for importing the certificate files:<br>• `REST_KEY_FILE`<br>• `REST_CRT_FILE`<br>• `SIP_KEY_FILE`<br>• `SIP_CERT_FILE`<br>• `OAM_KEY_FILE`<br>• `OAM_CRT_FILE`<br>• `NODE_KEY_FILE`<br>• `NODE_CRT_FILE`<br>• `CA_CRT_FILE` |

*Table continues…*

| Item name | Description | Equivalent `installation.properties` file parameter |
|---|---|---|
| **Local frontend host** | The local FQDN of the node.<br>The configuration utility uses this value to generate certificates for the node.<br>**Important:**<br>In a clustered configuration, the local front-end host is different from one node to the other and is also different from the front-end FQDN. In a non-clustered environment, the local front-end host is usually different from the front-end FQDN to create a clustered configuration from a non-clustered configuration. | `LOCAL_FRONTEND_HOST` |
| **Keystore password** | The keystore password for the MSS and Tomcat certificates.<br>The minimum length for this password is 6 characters. The characters supported for the keystore password are: | `KEYSTORE_PW` |

# LDAP configuration

If you do not complete LDAP configuration during the initial Avaya Aura® Web Gateway setup, then you can complete it later using the Avaya Aura® Web Gateway administration portal. Some administration options, such as configuring multiple LDAP directories, are only available on the administration portal. For more information, see *Administering the Avaya Aura® Web Gateway*.

**Warning:**

Changing the LDAP configuration parameters, other than Bind DN and Bind Credential, when they are configured, might invalidate the existing user data. For example, changing how user roles are found can remove one or more roles from the existing user, which will block the user from accessing the Avaya Aura® Web Gateway system. In addition, do not change the server URL unless you need to switch the configuration to another replicated instance of the current LDAP directory. In all the other cases, you must reinstall the Avaya Aura® Web Gateway system.

| Item name | Description | Equivalent properties file parameter |
|---|---|---|
| **Load LDAP properties from file** | The **Load LDAP properties from file** menu contains an item called **Path to properties file**. | pathToLdapPropertiesFile |

*Table continues…*

| Item name | Description | Equivalent properties file parameter |
|---|---|---|
| | You can create a Java properties file that contains the LDAP properties instead of entering the LDAP configuration settings manually. The **Path to properties file** option is for configuring the absolute path to this file.<br><br>The LDAP properties file must contain the *equivalent properties file parameters* specified in this table.<br><br>The default value for this setting is `<install_dir>/config/ldap.properties`, where `<install_dir>` is the installation directory. | |
| **Import Secure LDAP trusted certificate** | The **Import Secure LDAP trusted certificate** menu contains the following items:<br><br>• **Certificate file**: The path and filename for the LDAP trusted certificate. The certificate file must be in the .PEM format.<br><br>If you want to configure secure LDAP for onboard Open LDAP, use the nginx certificate located at `/etc/openldap/certs/nginx.crt`.<br><br>**Important:**<br><br>Only configure these settings if you need a Secure LDAP connection. | LDAP_TRUSTSTORE_CERTFILE<br><br>LDAP_TRUSTSTORE_PASSWORD |
| **Directory Type** | The LDAP directory type of the enterprise.<br><br>The supported directory types are the following:<br><br>• Microsoft Active Directory 2012, 2016, and 2019<br><br>• Microsoft Active Directory Lightweight Directory Services (AD-LDS)<br><br>• IBM Domino Server 7.0<br><br>**Note:**<br><br>The Domino server must be patched to support TLS, so Avaya Aura® Web Gateway can connect | ldapType |

*Table continues…*

| Item name | Description | Equivalent properties file parameter |
|---|---|---|
| | to the Domino server through secure LDAP (LDAPS). For a list of supported patch fixes, see https://www-10.lotus.com/ldd/dominowiki.nsf/dx/IBM_Domino_TLS_1.0.<br>• Novell e-Directory 8.8<br>• OpenLDAP 2.4<br>• Oracle Directory Server Enterprise Edition 11g Release 1 (11.1.1.7.0)<br>For detailed information about supported product releases, see the Avaya Compatibility Matrix. | |
| **URL for LDAP server** | The URL for gaining access to the LDAP server. This is the mandatory setting.<br>The URL must have one of the following formats:<br>`ldap://<LDAP server FQDN or IP address>:<port>`<br>`ldaps://<LDAP server FQDN>:<port>`<br>For example:<br>`ldap://myserver.mycompany.com:3268`<br>`ldaps://myserver.mycompany.com:3269`<br>The protocol can be LDAP or LDAPS, depending on the LDAP server type. If you are using LDAPS, you cannot use IP addresses in the URL.<br>**Important:**<br>If FIPS is enabled, use the LDAPS protocol to access the LDAP server.<br>For Microsoft Active Directory, use the catalog LDAP ports.<br>The default global catalog LDAP port values are 3268 for LDAP and 3269 for LDAPS.<br>The default domain LDAP ports values are 389 for LDAP and 636 for LDAPS. | ldapUrl |

*Table continues…*

| Item name | Description | Equivalent properties file parameter |
|---|---|---|
| | **Note:**<br>If an FQDN is used to specify the LDAP server, the enterprise might map the FQDN to multiple, replicated LDAP servers using the DNS round-robin mechanism as an attempt for load-balance and for redundancy purpose. Sporadic authentication failures can occur if one of the LDAP servers is offline and the DNS round-robin mechanism resolves the FQDN to the IP of the LDAP server that is offline.<br>If this outcome cannot be tolerated, a more reliable load-balancing mechanism, such as a dedicated load-balancer in front of the LDAP servers, will be needed.<br>For Active Directory, use the Global Catalog service port instead of the default LDAP/LDAPS ports.<br>**Important:**<br>If you are using the global catalog ports, you must configure attribute replication to the global catalog. For more information, see LDAP attributes replication to the global catalog on page 127. | |
| **Bind DN** | The Distinguished Name (DN) of the user that has read and search permissions for the LDAP server users and roles. This is the mandatory setting.<br>The format of the Bind DN depends on the configuration of the LDAP server.<br>**Note:**<br>Even though the parameter name is Bind DN, the format of its value is not limited to the DN format. The format can be any format that the LDAP server can support for LDAP bind. | bindDN |

*Table continues…*

| Item name | Description | Equivalent properties file parameter |
|---|---|---|
| | For example: for Active Directory, you can use `domain\user`, `user@domain`, as well as the actual DN of the user object. | |
| **Bind Credential** | Specifies the password of the administrative user.<br>The password length can be from 1 to 20 characters. | **Important:**<br>If you configure the LDAP settings using the properties file, you must enter the Bind Credential manually by running the **`configureCSA.sh`** script. |
| **UID Attribute ID** | The User ID attribute name, as determined by the LDAP server configuration. This is the mandatory setting.<br>This parameter is used for searching users in the LDAP server.<br>For example: `sAMAccountName` | uidAttrID |
| **Base Context DN** | The DN of the context used for LDAP authentication.<br>For example: `ou=csasusers,dc=example,dc=com` | baseCtxDN |
| **Administrator Role** | The list of LDAP roles that match the Avaya Aura® Web Gateway Administrator role.<br>For example:<br>If the role is configured as `CSAAdmin,CSAxyz`, any user whose list of roles contains `CSAAdmin` or `CSAxyz` is mapped to the Avaya Aura® Web Gateway Administrator role.<br>**Note:**<br>The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user in order for the mapping of the LDAP roles to the Avaya Aura® Web Gateway application roles to succeed. | adminRole |

*Table continues…*

| Item name | Description | Equivalent properties file parameter |
|---|---|---|
| | **Important:**<br>To avoid situations when potential loss of credentials could impact the administration tasks, Avaya recommends creating more than one user account with administrator privileges. | |
| **Auditor Role** | The list of LDAP roles that match the Avaya Aura® Web Gateway Auditor role.<br>For example:<br>If the Auditor role is configured as `CSAAuditor,CSAxyz`, any user whose list of roles contains the `CSAAuditor` or `CSAxyz` role is mapped to the Avaya Aura® Web Gateway AUDITOR role.<br>**Note:**<br>The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user in order for the mapping of the LDAP roles to the Avaya Aura® Web Gateway application roles to succeed. | auditorRole |
| **User Role** | The list of LDAP roles that match the Avaya Aura® Web Gateway User role.<br>For example:<br>If the User role is configured as `CSAUser,CSAxyz`, any user whose list of roles contains the `CSAUser` or `CSAxyz` role is mapped to the Avaya Aura® Web Gateway USER role.<br>**Note:**<br>The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user for the mapping of the LDAP roles to the Avaya Aura® Web Gateway application roles to succeed. | usersRole |

*Table continues…*

| Item name | Description | Equivalent properties file parameter |
|---|---|---|
| **Services Administrator Role** | The list of LDAP roles that match the Services Administrator role.<br>For example:<br>If the User role is configured as `CSAUser,CSAxyz`, any user whose list of roles contains the `CSAUser` or `CSAxyz` role is mapped to the Avaya Aura® Web Gateway Services Administrator role.<br>**Note:**<br>The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user for the mapping of the LDAP roles to the Avaya Aura® Web Gateway application roles to succeed. | serviceAdminRole |
| **Services Maintenance and Support Role** | The list of LDAP roles that match the Maintenance and Support role.<br>For example:<br>If the User role is configured as `CSAUser,CSAxyz`, any user whose list of roles contains the `CSAUser` or `CSAxyz` role is mapped to the Avaya Aura® Web Gateway Maintenance and Support role.<br>**Note:**<br>The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the roles name found for a user for the mapping of the LDAP roles to the Avaya Aura® Web Gateway application roles to succeed. | serviceMaintenanceRole |
| **Security Administrator Role** | The list of LDAP roles that match the Avaya Aura® Web Gateway Security Administrator role.<br>For example: | securityAdminRole |

*Table continues…*

| Item name | Description | Equivalent properties file parameter |
|---|---|---|
| | If the role is configured as `CSASecurityAdmin,CSAxyz`, any user whose list of roles contains `CSASecurityAdmin` or `CSAxyz` is mapped to the Avaya Aura® Web Gateway Security Administrator role.<br>**Note:**<br>The values of the roles are case-sensitive when they are mapped to the application roles. So they must match exactly to the role name found for a user in order for the mapping of the LDAP roles to the Avaya Aura® Web Gateway application roles to succeed. | |
| **Advanced LDAP parameters** | The menu that contains advanced LDAP parameters to configure depending on the structure of the LDAP server. | |
| **Test User** | If you select testUser and select **Apply**, this option is used to validate the following LDAP settings:<br>• Verifies that the user is searchable with a given base DN and search filter.<br>• Lists the group to which the user belongs — user, administrator, or auditor.<br>• Validates the values for Role Attribute ID and Role Name Attribute.<br>• Verifies the Last Updated Time attribute, role filter syntax, and active users search filter syntax.<br>The configuration is not saved if any of these validations fail.<br>The testUser parameter is optional. If you do not specify a value, the system skips validation and directly saves the configuration in the database. | testUser |

## LDAP advanced parameters

The following table describes the settings in the Advanced LDAP parameters menu:

| Item name | Description | Equivalent properties file parameter |
|---|---|---|
| **Role Filter** | The string to use for role filtering. This is the mandatory setting.<br>The format of the string depends on the LDAP server configuration.<br>For example: `(&(objectClass=group)(member={1}))` | `roleFilter` |
| **Role Attribute ID** | The Role Attribute ID parameter has a different meaning, depending on the value of **Role Attribute Is DN**:<br>• If **Role Attribute Is DN** is set to true, this is the attribute that contains the DN used to find the object that contains the role name.<br>• If **Role Attribute Is DN** is set to false, this is the name of the attribute that contains the role name.<br>For example: `memberOf`<br>This is the mandatory setting. | `roleAttrID` |
| **Roles Context DN** | The Roles Context DN to use for searching roles.<br>The roles search in LDAP is performed by using the Roles Context DN in combination with the Role Filter.<br>For example: `ou=csasusers,dc=example,dc=com` | `rolesCtxDN` |
| **Role Name Attribute** | This parameter has a different meaning, depending on the value of **Role Attribute Is DN**:<br>• If **Role Attribute Is DN** is set to true, the value of the attribute set in **Role Attribute ID** is used to find the object that contains the role and this parameter stores the name of the attribute that contains the role name. | `roleNameAttrID` |

*Table continues…*

| Item name | Description | Equivalent properties file parameter |
|---|---|---|
| | • If **Role Attribute Is DN** is set to false, this parameter is ignored.<br>For example: `cn` | |
| **Role Attribute is DN (true/false)** | The setting to determine if the role attribute is stored in the DN or in another object.<br>If you set this parameter to `true`, the role is stored in the attribute defined by the **Role Name Attribute** parameter.<br>If you set this parameter to `false`, the role attribute of the user contains the name of the role. | `roleAttrIsDN` |
| **Role Recursion** | The setting to enable or disable role recursion.<br>For example: the user jsmith can be in the Sales group, which can be in the users group. In this case, Role Recursion must be set to true to permit role recursion. | `roleRecursion` |
| **Allow Empty Passwords (true/false)** | The setting to determine if empty passwords are allowed in the LDAP directory. | `allowEmptyPasswords` |
| **Search Scope (0 - 2)** | The setting to determine the scope of the role search.<br>The role search starts from the *Role Context DN* and uses the *Role Filter*. The search scope determines the depth of the search as follows:<br>• Level 0, also named OBJECT_SCOPE, indicates that the search is performed only on the named role context.<br>• Level 1, also named ONELEVEL_SCOPE, indicates that the search is performed directly under the named role context.<br>• Level 2, also named SUBTREE_SCOPE, indicates | `searchScope` |

*Table continues…*

| Item name | Description | Equivalent properties file parameter |
|---|---|---|
| | that the search is performed at the named role context and in the sub-tree rooted at the named role context. | |
| **Language used in Directory** | The language used in the LDAP directory.<br>The following languages are supported:<br>• Russian<br>• German<br>• Spanish<br>• English<br>• Korean<br>• French<br>• Portuguese<br>• Simplified Chinese<br>• Japanese<br>• Italian | `language` |
| **Active users search filter** | The search filter string used to identify active users.<br>If the LDAP server supports a method of determining whether a user is active, this setting must contain the attribute that determines if a user is active.<br>If this setting is not configured, the User Management component handles all the users as active users.<br>For example:<br>`(&(objectClass=user)(objectCategory=Person)(!(userAccountControl:1.2.840.113556.1.4.803:=2))).` | `activeUsersFilter` |
| **Last updated time attribute** | The attribute indicating the last time an LDAP object was modified, in the ASN.1 Generalized Time Notation. | `lastUpdatedTimeAttr` |

*Table continues…*

| Item name | Description | Equivalent properties file parameter |
|---|---|---|
| | The Avaya Aura® Web Gateway User Management component uses this attribute to identify updated users when synchronizing the user data with the LDAP server.<br><br>If this parameter is not configured, the User Management component compares the data of every user to the data that exists in the LDAP server.<br><br>**Note:**<br><br>Configuring this parameter improves the efficiency of the user synchronization process and reduces the traffic between the Avaya Aura® Web Gateway server and the LDAP server during user synchronization. | |
| **Load parameter defaults** | The script to load the default values for the parameters. | — |

## Multiple authentication and authorization domains

Before Release 3.4, you could configure multiple LDAPs and have multiple base contexts on each LDAP, but you could only use one of them for authorization and authentication. With the single authentication and authorization domain restriction in place, users had to be provisioned multiple times so they existed in the authentication and authorization domain and in the other LDAPs used for search.

As of Release 3.4, the multiple authentication and authorization feature removes the requirement for a single domain for authentication and authorization and facilitates the following deployments:

- A single LDAP infrastructure belonging to a single organization with multiple configured domains.
- Two distinct LDAP infrastructures belonging to two separate organizations.

The Avaya Aura® Web Gateway supports up to ten LDAP authentication and authorization domains.

When multiple directories are enabled for authentication, you must provide your FQDN to log in. For example: `username@avaya.com`. A short user name is not supported. If you do not have proper data in user name attributes, such as mail and userPrincipalName, you can assign a custom attribute that is used for the UID mapping of user names. All values in the custom attribute must be a fully qualified user name of the form `username@domain`, where `domain` must match one of the base context DNs defined for the LDAP.

During the initial Avaya Aura® Web Gateway installation procedure, you can configure only one LDAP server. If you want to add more LDAP servers, use the web administration portal. For more information, see “Adding a new enterprise LDAP server” in *Administering the Avaya Aura® Web Gateway*.

## Configuring the role search parameters

### About this task

This procedure describes how to configure the LDAP role search parameters when Microsoft Active Directory (AD) is used.

Role search for Avaya Aura® Web Gateway users are really about finding the associated “role” strings for a user in LDAP. For AD, this is about the user group names that a user belongs to.

In Microsoft Active Directory, the DNs of the groups that a user belongs to are stored in the “memberOf” attribute of a user. The “memberOf” attribute also stores the Exchange mailing lists that a user belongs to. Conversely, the group objects that the user belongs to contain a “member” attribute that stores the DNs of all of the users and sub-groups that are members of this group.

### Procedure

1. Run the Avaya Aura® Web Gateway configuration utility using the `app configure` command.
2. Select **LDAP Configuration** > **Advanced LDAP parameters**.
3. Configure the parameter settings as described in Parameter settings on page 124.
4. Configure the attributes as described in Role configuration on page 126.

## LDAP parameter descriptions

### Parameter settings

The following table describes the parameter settings according to the search mechanism that you choose:

| Parameter | Search mechanism #1:<br>Find the user, extract the group DNs from the "memberOf" attribute, and get the role strings from each of the group objects | | Search mechanism #2:<br>Find the groups that the user belongs to and extract the role string from one of the attributes | |
|---|---|---|---|---|
| | **Example** | **Description** | **Example** | **Description** |
| Role Filter | (&(objectClass=user)(objectCategory=Person)(<UID attribute ID>={0})) | <UID Attribute ID> is the value of the "UID Attribute ID" parameter.<br>"{0}" is the placeholder that will be replaced by the authenticating user ID. | (&(objectClass=group)(member={1})) | "{1}" is the placeholder to be replaced by the DN of the user object. The DN is identified during the authentication process.<br>This filter looks for a group object whose "member" attribute contains a value of the authenticating user DN. |
| Role Context DN | ou=Users,dc=global,dc=example,dc=com | The purpose of the search is to find the user and then extract the role objects from the "memberOf" user attribute. | ou=Groups,dc=global,dc=example,dc=com | The purpose of the search is to find the roles whose "member" attribute contains the user. |
| Role Attribute ID | "memberOf" | This attribute contains the list of DNs of the groups to which the user belongs to. | CN | This contains the group's name (e.g. "AAWGAdmin", etc.) |
| Role Attribute is DN | true | The "memberOf" values are the DNs of the group/mailing list objects. | false | The "Role Attribute ID" already contains the "role" string name. |
| Role Name Attribute | CN | The attribute defined by Role Name Attribute contains the group name.<br>For example: AAWGAdmin | | Leave this empty because "Role Attribute is DN" is false. |

*Table continues…*

| Parameter | Search mechanism #1:<br>Find the user, extract the group DNs from the "memberOf" attribute, and get the role strings from each of the group objects | | Search mechanism #2:<br>Find the groups that the user belongs to and extract the role string from one of the attributes | |
|---|---|---|---|---|
| | Example | Description | Example | Description |
| Role Recursion | 0 | This configuration does not allow recursive search.<br>**Note:**<br>Using this configuration, the users under the "AAWGDelegates" group will not be able to use Avaya Aura® Web Gateway so this is not the recommended configuration for this example. | 1 or higher | You must set this value to 0 if there are no subgroups or a value from 1 to 10 to support searches of users that are in subgroups.<br>In this example, the recursive search is needed to find the user in the "AAWGDelegates" group, so this value must be set to at least 1. |

## Role configuration

To search the role base context and under it, set **Search Scope** to `2` or `SUBTREE_SCOPE` . The configuration of the following roles is the same, regardless of the configured search mechanism:

| Role | Description | Example |
|---|---|---|
| Administrator Role | This role specifies the list of the "role" string extracted from LDAP that would be mapped to the Avaya Aura® Web Gateway server ADMIN application role. | AAWGAdmin |
| User Role | This role specifies the list of the "role" string extracted from LDAP that would be mapped to the Avaya Aura® Web Gateway server USERS application role. | AAWGUsers |
| Auditor Role | This role specifies the list of the "role" string extracted from LDAP that would be mapped to the Avaya Aura® Web Gateway server AUDITOR application role. | AAWGAuditor |
| Service Administrator Role | Avaya Aura® Web Gateway does not currently use this role. Leave this setting blank. | |
| Services Maintenance and Support Role | Avaya Aura® Web Gateway does not currently use this role. Leave this setting blank. | |
| Security Administrator Role | This role is for updating web certificates from the web administration portal. | AAWGSecurityAdmin |

## LDAP attributes replication to the global catalog

If you are using global catalog ports 3268 or 3269 to connect to LDAP, then LDAP queries can only return attributes marked for replication to the global catalog. For example, a user's department cannot be returned because this attribute is not replicated to the global catalog. You must manually add all required attributes in the global catalog attributes list.

# Cluster configuration

Using the Cluster configuration, you can configure the Avaya Aura® Web Gateway nodes in a clustered environment.

| Item name | Description | Equivalent `installation.properties` file parameter |
|---|---|---|
| **Initial cluster node** | The setting to specify if the server where you are performing the installation is the initial node in a cluster.<br>Select `y` (yes) to set the current node as the initial node in the cluster or `n` (no) to set the current node as an additional node.<br>The default value for this setting is `y` (yes).<br>In a standalone installation, set this value to `y` (yes).<br>If you configure this setting to `n` (no), the following settings become visible and must be configured:<br>• The IP address of the initial cluster node.<br>• The ID of the Linux user performing the installation on the initial node.<br>• The Cassandra database user name for the initial node.<br>• The Cassandra database password for the initial node. | `INITIAL_NODE`<br>If you configure this setting to `n` (no), you must also configure the following parameters:<br>• `SEED_NODE`<br>• `REMOTE_UID`<br>• `CURRENT_CASSANDRA_USER`<br>• `CURRENT_CASSANDRA_PASSWORD` |
| **Local node IP address** | The IP address of the local node. | `CLUSTER_IP_ADDR` |

# Virtual IP configuration options

| Option | Description | Equivalent `installation.properties` file parameter |
|---|---|---|
| **Enable virtual IP** | The setting to enable the usage of a virtual IP address.<br>If you select `n` (no), the configuration script does not configure the virtual IP address.<br>If you select `y` (yes), new configuration settings for the virtual IP address are displayed in the configuration menu. These settings are listed below in this table. If you are performing a silent installation you must also configure these parameters in the `installation.properties` file. | `KA_ENABLED` |
| **Virtual IP address** | The virtual IP address shared by all the cluster nodes. | `KA_VIRTUAL_IP` |
| **Virtual IP interface** | The network interface used for the virtual IP address. Unless you are using a configuration that has multiple Ethernet interfaces, you must set this value to `eth0` (Ethernet-zero). | `KA_INTERFACE` |
| **Virtual IP master node** | Determines if the current node is the virtual IP master node. As the initial node of the cluster is usually designated the virtual IP master, set this value to `y` (yes), on the initial node. In addition, as the second node in a cluster is usually designated the virtual IP backup, set this value to `n` (no) on the second node. | `KA_MASTER_YN` |
| **Virtual IP router ID** | An integer with a value from 1 to 255. The value must be the same for both virtual IP master and backup. The default value is 71.<br>This value must be unique across Virtual Router Redundancy Protocol (VRRP) installations. | `KA_ROUTER_ID` |
| **Virtual IP authentication password** | The password that the backup node uses for authentication. This password must be the same as the virtual IP authentication password configured for the initial node. | `KA_AUTHENTICATION_PASSWORD` |

**Related links**

Avaya Aura Web Gateway initial configuration settings on page 108

# Advanced configuration

**Table 4: Advanced configuration settings**

| Item name | Description | Equivalent `installation.properties` file parameter |
|---|---|---|
| **Certificate Warning Period** | The number of days before the expiry date of a certificate causes the system to raise an alarm. | `CERT_WARNING_PERIOD` |
| **OS Security Utility** | The menu for configuring the firewall automatically on the current node.<br>Select **Run the firewall configuration script** and press Enter to run the firewall configuration script.<br>Avaya recommends that you run this script to configure the firewall automatically and not perform a manual configuration.<br>**Warning:**<br>The firewall configuration script replaces the current configuration of the firewall on the server where you are performing the installation, so you must open any other ports required for your server manually after you run this script. | `RUN_FIREWALL_CONFIG`<br>If you set this parameter to `y` (yes), the firewall configuration script is run during the silent installation. |
| **Long Poll Timeout** | The menu that contains the **Recommended Long Poll Timeout** configuration option. Use this option for setting the value to use in the Avaya-Request-Timeout HTTP header for long-poll requests.<br>**Important:**<br>The long poll timeout value can be from 30 to 120. Lowering this value results in increased traffic on the server, but network configuration may require that you set a lower value. | `AVAYA_REQUEST_TIMEOUT` |

*Table continues…*

| Item name | Description | Equivalent `installation.properties` file parameter |
|---|---|---|
| | If you do not configure this parameter, the default database initialization setting is used. | |
| **Configure Host IP for SNMP management** | The menu that contains the **IP address for managing this server** setting for configuring the IP address of the Network Interface to use for SNMP. | `SNMP_IP_ADDR` |
| **Security Banner File** | The menu for configuring security banner settings.<br>The **Security Banner File** setting must contain the path to the security banner file.<br>The security banner file is a text file that contains the security warnings displayed when a user or administrator logs in to the administration portal or using an SSH console. | `SECURITY_BANNER_PATH` |

# Changing the Cassandra user name and password

## About this task

After installing the Avaya Aura® Web Gateway application, you must change the default Cassandra database password to comply with the security requirements.

This procedure describes how to change the Cassandra database user name and password after installing of an Avaya Aura® Web Gateway cluster.

## Before you begin

Install the Avaya Aura® Web Gateway application. If you install an Avaya Aura® Web Gateway cluster, install all cluster nodes before changing the Cassandra database password.

## Procedure

1. On the seed node, do the following:
   a. Log in to the Avaya Aura® Web Gateway CLI as an administrator.
   b. Run the Avaya Aura® Web Gateway configuration utility using the following command:
      ```
      app configure
      ```
   c. Select **Cassandra DB User and Password**.
   d. Select **New Cassandra Database User Name** and enter the new user name.
   e. Select **New Cassandra Database User Password** and enter the new password.
   f. Select **Apply**.

2. In a cluster deployment, on every non-seed node, do the following:
   a. Log in to the Avaya Aura® Web Gateway CLI as an administrator.
   b. Run the **cassandraSetPassword** command and specify the new password and user name as parameters.

      ```
      sudo /opt/Avaya/CallSignallingAgent/<verion>/CAS/<verion>/cassandra/
      cassandraSetPassword.sh <new user name> <new password>
      ```

   c. Restart Avaya Aura® Web Gateway.

      ```
      svc csa restart
      ```

# Changing the default password for automatic backups

### About this task

Avaya recommends that you change the default password that Avaya Aura® Web Gateway uses for automatic backups.

### Procedure

1. Log in to the Avaya Aura® Web Gateway web administration portal at `https://<AADS FQDN or IP>:8445/admin/`.

   For more information about the login procedure, see “Logging in to the Avaya Aura® Web Gateway web administration portal” in *Administering the Avaya Aura® Web Gateway*.
2. Go to **Automatic Backup Configuration**.
3. Select the **Change Password** check box.
4. In **Backup File Password**, type a new password.

   The password must comply with the password complexity rules. You can view the rules by pointing the cursor to the **Backup File Password** field.
5. In **Re-Enter Password**, type the password again.
6. Click **Save**.

# Starting services using a command line

### About this task

Use this procedure to start application services after you complete installation.

### Procedure

1. Open the Linux shell using your Linux administrator account credentials.

   The Linux administrator account is created during the deployment process.

2. To start the Avaya Aura® Web Gateway services, run the following command:

```
svc csa start
```

# Configuring OAMP to use Linux account credentials on the Avaya Aura® Web Gateway administration portal

## About this task

This is an optional procedure that you need to perform if you want to log on to the Avaya Aura® Web Gateway administration portal using Linux account credentials.

## Procedure

1. Open the Linux shell using your Linux administrator account credentials.

   The Linux administrator account is created during the deployment process.

2. Run the following command:

```
cdto active
sudo vi tomcat/<tomcatVersion>/conf/catalina.properties
```

3. Locate the `com.avaya.cas.access.groups` properties and update the list of groups allowed to access the web administration portal as required.

   Ensure that entries in the group list are separated by a comma. The following is an example:

```
# OAMP access linux groups
com.avaya.cas.access.groups.admin=admingrp
com.avaya.cas.access.groups.securityadmin=admingrp
```

   Users that are part of the “admingrp ” group have access to the web administration portal by default.

4. Run the following command to apply the changes:

```
svc tomcat restart
```

# Chapter 7: Global FQDN configuration

You can use a single FQDN for all services or multiple FQDNs for each service. If you are using multiple FQDNs, you require an external interface on the reverse proxy for each FQDN and separate certificates for each FQDN.

In a single FQDN environment, remote clients and endpoints that participate in conferences interact with multiple components through HTTPS. To eliminate the need for multiple external public IPs, FQDNs, and certificates, the URL rewriting method is used. Using this method, clients and endpoints can access conferences using a single FQDN and a single IP address through port 443.

## DNS configuration

- For a single FQDN deployment, configure DNS as follows:
  - For external DNS configuration, have a single FQDN record, for example, `webservices.company.com`, that points to the reverse proxy or load balancer interface for external traffic.
  - For internal DNS configuration, have a single FQDN record, for example, `webservices.company.com`, that points to the reverse proxy or load balancer interface for internal traffic.
- For a multiple FQDNs deployment, configure DNS as follows:
  - For external DNS configuration, each FQDN points to the external load balancer interface.
  - For internal DNS configuration, each FQDN points to the individual server components.

**Related links**

Required FQDNs and certificates on page 29

## Configuring the front-end FQDN

**Procedure**

1. Log in to the Avaya Aura® Web Gateway administration portal.
2. Navigate to **External Access** > **HTTP Reverse Proxy**.
3. Configure the following settings:

4. In **Host**, provide the service FQDN.

   For example: You can use `webservices.company.com` in a single FQDN deployment. In a multiple FQDN deployment, use `webgateway.company.com`.

5. In **Port**, enter `443`.
6. If you have any external clients, including WebRTC, mobile, or desktop clients outside the enterprise firewall, do the following to enable a remote port:
   a. Select the **Enable port for external access** check box.
   b. In **Front-end port for external access**, enter a value between 1024 and 65535.

      The default port value is 8444.

   This port setting must be configured in the reverse proxy so traffic for clients outside the firewall is translated from the front-end port to this remote access port.
7. If you are configuring a geographically distributed system, select the **Enable use of an external load balancer** check box.
8. Click **Save**.

**Related links**

Geographical distribution overview on page 15

# Avaya Meetings Server configuration for single FQDN deployments

## Configuring Avaya Workplace Client conference control

### Procedure

1. Log in to the Avaya Meetings Management web administration portal.
2. Navigate to **Settings** > **Advanced Parameters**.
3. In **Property Name**, enter `com.visionnex.vcms.core.uccp.customizedUCCPURL`.
4. In **Property Value**, enter `https://<Service FQDN>:443/uwd/ws?ticket=`.

   For example: `https://webservices.company.com:443/uwd/ws?ticket=`.

5. Click **Apply**.

# Configuring Web Collaboration

### Procedure

1. Log in to the Avaya Meetings Management web administration portal.
2. Navigate to **Devices** > **Devices by Type** > **<Web Collaboration server name>** > **Configuration**.
3. Configure the following settings:
   a. In **Service FQDN** and **Local FQDN**, enter the service FQDN that resolves to the IP address of the selected Web Collaboration node.

      For example: `webconference1.company.com`

   b. In **IP Address**, enter the IP address that is resolved from the service and local FQDNs.

   c. In **Public URL Branch**, enter `<Service FQDN>/<Web Collaboration Services node prefix>`.

      For example: `webservices.company.com/webconference1`.

      **Note:**

      The public branch URL is used to support multiple Web Collaboration Services nodes with a single public FQDN.
4. Repeat the previous steps for each Web Collaboration Services server that is part of the deployment.

# Chapter 8: System Manager, Avaya Aura® Device Services, Media Server, and Avaya Meetings Server configurations

## Adding the Avaya Aura® Web Gateway to System Manager

### About this task

Use this procedure to enable SSO login and add the Avaya Aura® Web Gateway FQDN to the System Manager web console.

**Note:**

To set up an Avaya Aura® Web Gateway cluster, use the front-end FQDN for the cluster. If you are using an external load balancer, the front-end FQDN for the cluster will be the FQDN of the load balancer. If not, it will be the FQDN of the virtual IP assigned to the Avaya Aura® Web Gateway cluster.

### Before you begin

Ensure that you have administrative privileges to access System Manager.

For information about accessing System Manager, see *Administering Avaya Aura® System Manager*.

### Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **New**.

   The system displays the New Elements page.
4. In the General section, from **Type**, select **Avaya Aura Web Gateway** .
5. On the New Avaya Aura Web Gateway page, in the General section, provide the following information:
   - **Name**: Type a name for the element.
   - **Type**: Retain the default setting of **Avaya Aura Web Gateway**.

- **Description**: Type a description for the element.
- **Node**: Type the FQDN address of the Avaya Aura® Web Gateway server.

6. To enable SSO login, in the Access Profile section, perform the following:
   a. Click **New**.
   b. In the Application System Supported Protocol section, in the **Protocol** field, click **URI**.
   c. In the Access Profile Details section, in the **Name** field, type a name for the access profile.
   d. In the **Access Profile Type** field, click **EMURL**.
   e. In the **Protocol** field, click **https**.
   f. In the **Host** field, type the Avaya Aura® Web Gateway server FQDN.
   g. In the **Port** field, type `8445`.
   h. In the **Path** field, type `/admin`.
   i. In the **Order** field, retain the default value.
   j. In the **Description** field, type a description of the access profile.
   k. Click **Save**.
7. Click **Commit**.
8. On the System Manager console, click **Elements** > **Web Gateway** to verify that the Avaya Aura® Web Gateway element has been added.

# Configuring SIP Trunks for the Avaya Aura® Web Gateway on System Manager

## About this task

The Avaya Aura® Web Gateway sends SIP messages to Session Manager port 5061 using TLS. Use this procedure to ensure that Session Manager is configured to accept these messages.

**Important:**

For an Avaya Aura® Web Gateway cluster, repeat this procedure for each node in the cluster using the respective node IP or local FQDN when required.

## Before you begin

Set up your Avaya Aura® infrastructure, including System Manager.

## Procedure

1. On the System Manager web console, click **Elements** > **Routing** > **SIP Entities**.
2. In the SIP Entities area, click **New** to create a new SIP entity for your server.

   You can also edit an existing SIP entity using the **Edit** button.

3. On the SIP Entity Details page, configure the following required field settings:
   - **Name**: Type a name for the SIP entity.
   - **FQDN or IP Address**: Type the FQDN or IP address of the Avaya Aura® Web Gateway.
   - **Type**: Select **SIP Trunk**.
   - **SIP Timer B/F (in seconds)**: Retain the default value of 4.
   - **SIP Link Monitoring**: Select **Link Monitoring Disabled**.

   For information about other fields, see the SIP entity field descriptions in *Administering Avaya Aura® Session Manager*.
4. In the Entity Links area, click **Add** to add entity links between the newly created SIP entity and the entities representing Session Manager.

   While mapping the newly created SIP entity with the Session Manager entities, ensure that the following is set:
   - **Protocol**: **TLS**.
   - **Port**: **5061**.
   - **Connection Policy**: **trusted**.
5. Click **Commit** to save the changes.

# Serviceability agents

You must set up serviceability agents to receive Avaya Aura® Web Gateway alarms in System Manager. To configure serviceability agents, set up an SNMPv3 user profile and an SNMP target profile. Then assign the SNMPv3 user profile to the SNMP target profile.

For more information about managing serviceability agents, see *Administering Avaya Aura® System Manager*.

## Setting up an SNMPv3 user profile

### About this task

An SNMPv3 user profile enables you to define privileges so serviceability agents can read and write data in SNMP Management Information Bases (MIBs).

### Procedure

1. On the System Manager web console, navigate to **Services** > **Inventory** > **Manage Serviceability Agents** > **SNMPv3 User Profiles**.
2. In the User Details section, click **Edit**.
3. In the **User Name** field, type `initial`.
4. In the **Authentication Protocol** field, select **SHA**.

   The **MD5** setting is not supported.

5. In the **Authentication Password** field, type the authentication password.

   The default authentication password is `avaya123`.
6. In the **Confirm Authentication Password** field, confirm the password.
7. In the **Privacy Protocol** field, select **AES**.
8. In the **Privacy Password** field, type the privacy password.

   The default privacy password is `avaya123`.
9. In the **Confirm Privacy Password** field, confirm the password.
10. In the **Privileges** field, select **Read/Write**.
11. Click **Commit**.

## Setting up an SNMP target profile

### About this task

An SNMP target profile contains settings for sending alarms from Avaya Aura® Web Gateway to System Manager.

### Procedure

1. On the System Manager web console, navigate to **Services** > **Inventory** > **Manage Serviceability Agents** > **SNMP Target Profiles**.
2. On the Target Details tab, click **Edit**.
3. In the **Name** field, type the name of the profile.
4. In the **Description** field, type a description for the profile.
5. In the **IP Address** field, type the System Manager IP address.
6. In the **Port** field, type `10162`.
7. In the **Notification Type** field, select **Trap**.
8. In the **Protocol** field, select **V3**.
9. Click **Commit**.

## Assigning the SNMPv3 user profile

### About this task

You must assign the SNMPv3 user profile to the target profile so System Manager can receive alarms from Avaya Aura® Web Gateway.

### Before you begin

Set up an SNMPv3 user profile and an SNMP target profile.

### Procedure

1. On the System Manager web console, navigate to **Services** > **Inventory** > **Manage Serviceability Agents** > **Serviceability Agents**.

2. Select the Avaya Aura® Web Gateway host name, and click **Manage Profiles**.
3. Click the **SNMP Target Profiles** tab.
4. In the Assignable Profiles section, click the SNMP target profile you created, and click **Assign**.
5. Click the **SNMPv3 User Profiles** tab.
6. In the Assignable Profiles section, select the SNMPv3 profile you created, and click **Assign**.
7. Click **Commit**.

## Configuring a registration expiration timer

### About this task

The Registration Expiration Timer setting in Session Manager defines a time interval for a SIP server to keep SIP clients registered. Avaya Aura® Web Gateway receives this value from Session Manager and uses it as a refresh interval for SIP registration. The minimal refresh interval supported by Avaya Aura® Web Gateway is 600 seconds or 10 minutes. You must ensure that the Registration Expiration timer in Session Manager is set to at least 600 seconds.

### Procedure

1. In System Manager, navigate to **Elements** > **Session Manager** > **Device and Location Configuration** > **Device Settings Groups**.
2. Select the appropriate Device Settings Group.

   If no additional groups were created, select **Default Group**.
3. In the Server Timer section, ensure that the **Registration Expiration Timer Minimum** value is set to at least 600 seconds.

## Configuring Avaya Aura® Media Server in System Manager

### About this task

This procedure outlines the key System Manager configuration required for the Media Server. Use this procedure to administer locations for all Media Server clusters and assign the Endpoint Services Gateway to each Media Server cluster.

**Note:**

Avaya Aura® Web Gateway does not support Media Server High Availability cluster configuration when using WebRTC.

### Procedure

1. Enroll all Media Server clusters in System Manager.

The enrollment must be done using a System Manager account with administrative privileges for adding, changing, deleting, and viewing all Media Server element types. By doing this, the configuration of the Media Server and the nodes within the cluster will be available on the System Manager server. The Media Server must be enrolled with System Manager release 7.0.1.1 or higher. For more information about System Manager enrollment, see *Implementing and Administering Avaya Aura® Media Server*.

2. Administer locations for all Media Server clusters.
   a. In System Manager, navigate to **Elements** > **Media Server** > **Server Administration**.
   b. In each required Media Server, set the location.

   For more information about Media Server clusters location setting, see *Managing Avaya Aura® Media Server from System Manager*.
3. Assign “Endpoint Services Gateway” to each cluster of Media Server that will be used by the Avaya Aura® Web Gateway.
   a. In System Manager, navigate to **Elements** > **Media Server** > **Application Assignment**.
   b. Edit the “Endpoint Services Gateway” application.
   c. Select the required Media Server clusters.

   For more information about Media Server cluster location settings, see *Managing Avaya Aura® Media Server from System Manager*.

# Configuring Avaya Aura® Media Server settings

## About this task

This procedure describes how to configure Avaya Aura® Media Server to enable Interactive Connectivity Establishment (ICE) and video processing.

**Note:**

For performance reasons, Avaya recommends that you use the client-side TURN service. Use server-side TURN only if you cannot use client-side TURN due to your deployment limitations.

For more information about setting up Avaya Aura® Media Server, see *Implementing and Administering Avaya Aura® Media Server*.

## Before you begin

Ensure that WebLM server licensing is configured and enabled in Avaya Aura® Media Server.

## Procedure

1. Log on to the Avaya Aura® Media Server Element Manager using the URL `https://<AMS_EM_FQDN>:8443/emlogin/`.
2. Navigate to **System Configuration** > **Server Profile** > **General Settings**.

3. Select **Firewall NAT Tunneling Media Processor** and **Video Media Processor** and then click **Save**.
4. Navigate to **System Configuration** > **Signaling Protocols** > **REST** > **General Settings**.
5. Select **Enable TLS Mutual Authentication** and click **Save**.
6. Do the following to enable the TURN service on the client side:
   a. Log in to the Avaya Aura® Web Gateway administration portal.
   b. Navigate to **External Access** > **Session Border Controller**.
   c. elect the **Enable TURN in WebRTC client** check box.
   d. On the Avaya Aura® Media Server Element Manager, navigate to **System Configuration** > **Media Processing** > **ICE** > **STUN/TURN Servers**.
   e. Ensure that all STUN and TURN servers are disabled.

   For more information about enabling client side TURN for the WebRTC clients, see the sections in WebRTC client side TURN configuration on page 164.
7. **(Optional)** If you cannot use client-side TURN in your deployment, do the following to enable server-side TURN:
   a. on the Avaya Aura® Media Server Element Manager, navigate to **System Configuration** > **Media Processing** > **ICE** > **STUN/TURN Servers**.
   b. Select the required STUN and TURN servers.

   **Tip:**

   You can verify the network configuration when you are using Avaya Session Border Controller for Enterprise (Avaya SBCE) to provide the STUN/TURN service. The STUN/TURN address and port configured on the media server must match the STUN/TURN Listen IP & Listen port that are configured for the A1 interface of the Avaya SBCE. You must also use the default values for the following settings:

   - Protocol: `UDP`.
   - Priority: `0`.
   - Weight: `10`.
   - Account: `disabled`.
8. Navigate to **Licensing** > **General Settings** and ensure that WebLM server licensing is enabled.
9. Navigate to **Licensing** > **Monitoring** and ensure that Avaya Aura® Media Server has acquired licenses.
10. For the changes to take effect, navigate to **System Status** > **Element Status** and click **Restart**.

# Configuring the Avaya Aura® Web Gateway on Avaya Aura® Device Services

### About this task

Use this procedure to add the Avaya Aura® Web Gateway FQDN to the Avaya Aura® Device Services trusted hosts and to verify HTTP client settings.

For more information about Avaya Aura® Device Services, see the following documents:

- *Deploying Avaya Aura® Device Services*
- *Administering Avaya Aura® Device Services*

### Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections** > **Trusted Hosts** and click **Add**.
2. In **Host**, type the Avaya Aura® Web Gateway FQDN.

   **Important:**

   Avaya Aura® Device Services requires the FQDN or IP address for each Avaya Aura® Web Gateway cluster node added to the Avaya Aura® Device Services trusted hosts list. Avaya Aura® Device Services also requires the FQDN or IP address of the Avaya Aura® Web Gateway cluster.
3. On the **HTTP Clients** tab, ensure that the **REST** and **OAMP** options are not set to `NONE`.

   If these options are set to `NONE`, then the trusted host relationship between the Avaya Aura® Web Gateway and Avaya Aura® Device Services will not work. The Avaya Aura® Web Gateway will also not be able to communicate with Avaya Aura® Device Services.

# Uploading clients to the web deployment service

### About this task

Use this procedure to upload Windows and MacOS clients to the web deployment service.

For Avaya Workplace Client for Windows, you can upload `.exe` or `.msi` installation files. For Avaya Workplace Client for Mac, you can upload `.dmg` installation files, which are packaged in a `.zip` archive.

**Note:**

This procedure applies to Team Engagement and Conferencing deployments. This document does not describe the Conferencing-only deployment model.

For more information about web deployment client installers, see *Administering Avaya Aura® Device Services*.

### Procedure

1. Download Avaya Workplace Client for Mac or Avaya Workplace Client for Windows installation files from the Avaya Support website.

   **Note:**

   You must have PLDS access to download these files.

2. If you are uploading Avaya Workplace Client for Mac, pack the `Avaya Equinox-<version>.dmg` and `Avaya Equinox Sparkle Update-<version>.dmg` files into a `.zip` archive with no intermediate directories.

   If the `.zip` archive contains intermediate directories, re-pack the archive so that it only contains the `.dmg` files in the root directory.

3. Log on to the Avaya Aura® Device Services web administration portal and navigate to **Web Deployment** > **Deployment**.
4. In **Title**, type a name of the updates or appcast for the client installer.
5. In **Description**, type the description of the client installer updates.
6. In **Version**, type the version details for the Avaya Workplace Client release.
7. In **OS**, select the appropriate Avaya Workplace Client platform:
   - Windows
   - Macintosh
8. In **File**, click **Choose File** and select one of the following files to upload:
   - For Avaya Workplace Client for Windows, select the `.exe` or `.msi` installation file.
   - For Avaya Workplace Client for Mac, select the `.zip` archive containing the `.dmg` installation files.

# Configuring the Avaya Aura® Web Gateway on Avaya Meetings Server

### About this task

If your deployment includes Conferencing, use this procedure to perform the required configuration on the Avaya Meetings Server Management portal. For more information about Conferencing configuration, see *Deploying Avaya Meetings Server*.

**Important:**

- For the Avaya Aura® Web Gateway and Avaya Meetings Server to establish a secure connection, each must trust the Root CA that signed the other's certificates. If the System Manager signed certificates are applied in Avaya Meetings Server, no further action is required on the Avaya Aura® Web Gateway.

If the certificates applied in Avaya Meetings Server are signed by a third-party CA other than System Manager, you must follow the steps outlined in Adding third-party root CA certificates to the Avaya Aura Web Gateway on page 191. For more information about certificates in Avaya Meetings Server, see *Administrator Guide for Avaya Meetings Management*.

- A separate User Portal device must be added for each node on the Avaya Aura® Web Gateway cluster using its respective IP address and location.

### Procedure

1. Log on to the Avaya Meetings Server Management portal.
2. Do the following to add the Avaya Aura® Web Gateway server as a managed server device on Avaya Meetings Server:
   a. Navigate to **Devices** > **User Portals**.
   b. To add the Avaya Aura® Web Gateway server to the list, click **Add**.

      The system displays the Add Management Server dialog box.
   c. Enter a unique display name and IP address of the server.
   d. From the **Location** drop-down menu, select location to match the Avaya Aura® Web Gateway location assignment on the Avaya Aura® Web Gateway administration portal.
   e. Click **OK**.
3. Wait for a few minutes until the newly added User Portal Device indicator changes from gray to green.

# Route configuration for an external load balancer

Reverse proxy and load balancer need to accept external and internal connections to the <Service FQDN>:443 address. For example: conferencing.avaya.com:443.

Usually, the Avaya Aura® Web Gateway uses its own internal load balancer that distributes requests between cluster nodes. The Avaya Aura® Web Gateway internal load balancer handles internal and external requests differently:

- Internal requests use port 443.
- External requests use port 8444.

When you use an external load balancer, it redirects internal requests to Avaya Aura® Web Gateway port 443 and external requests to Avaya Aura® Web Gateway port 8444.

The following table shows URL replacement methods that you must configure on the external load balancer to update requests to different servers and services.

| Request URL | Destination Address | URL Replace | Component |
|---|---|---|---|
| /uwd/rest | <Equinox Management Virtual IP FQDN>:443 | /uwd/rest | Avaya Workplace Client Conference Control (UCCS) |
| /uwd/ws | | /uwd/wc | |
| /wcs1/ | <WCS1 FQDN>:443 | / | Avaya Aura® Media Server |
| /wcs2/ | <WCS2 FQDN>:443 | / | |
| /wcsX/ | <WCSX FQDN>:443 | / | |
| /ups | • <AAWG Node 1 FQDN>:<port><br>• <AAWG Node 2 FQDN>:<port><br>• <AAWG Node X FQDN>:<port><br>For internal requests, use port 443. For external requests, use port 8444. | /ups | Avaya Aura® Web Gateway |
| /csa | | /csa | |
| /uwd/dist | | /uwd/dist | |
| /notification | | /notification | |
| /portal | | /portal | |
| /acs | • <AADS Node 1 FQDN>:8448<br>• <AADS Node 2 FQDN>:8448<br>• <AADS Node X FQDN>: 8448 | /acs | Avaya Aura® Device Services |

# Chapter 9: Avaya Session Border Controller for Enterprise configuration

Use the following sections to configure Avaya Session Border Controller for Enterprise (Avaya SBCE) for the Avaya Aura® Web Gateway. You require Avaya SBCE when you have clients located outside the enterprise firewall. For example, Avaya SBCE is required if you need remote worker functionality. Avaya SBCE is not required if all client users are on the private network within the enterprise firewall.

The Avaya Aura® Web Gateway can use the following services:

- Reverse proxy service, which handles HTTP or HTTPS traffic form outside the firewall into the internal network. Reverse proxy is placed on the DMZ and routes HTTP(S) traffic to the Avaya Aura® Web Gateway for external clients.
- TURN service, which is required when the Avaya Aura® Web Gateway interacts with browser-based audio and video clients outside the enterprise.
- Session border controller service, which is required for audio and video clients to make calls outside the enterprise.

Avaya Session Border Controller for Enterprise provides this functionality as an Edge device. You do not need a dedicated Avaya SBCE for Avaya Aura® Web Gateway. You can use any Avaya SBCE within the enterprise.

For more information about Avaya SBCE configuration, see *Administering Avaya Session Border Controller for Enterprise*.

**Related links**

Required FQDNs and certificates on page 29

## Avaya Session Border Controller for Enterprise configuration checklist

Perform the tasks in this checklist to configure Avaya SBCE.

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 1 | Ensure that you have a pool of IP addresses available for Avaya SBCE. | — | |
| 2 | Configure reverse proxy. | • In a single FQDN for all services deployment, complete the tasks outlined in Reverse proxy configuration checklist for a single FQDN deployment on page 148.<br>• In a multiple FQDN deployment, complete the tasks outlined in Reverse proxy configuration checklist for a multiple FQDN deployment on page 149. | |
| 3 | If you are planning to use external clients outside the enterprise firewall, configure external client access. | Complete procedures in External client access configuration on page 159. | |

# Reverse proxy configuration

## Reverse proxy configuration checklist for a single FQDN deployment

Perform the tasks outlined in this checklist to configure reverse proxy on the Avaya SBCE if you are using a single FQDN for all services.

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 1 | Verify prerequisites. | See Prerequisites on page 149. | |
| 2 | Create a TLS server profile for reverse proxy. | See Checklist for creating a TLS server profile for reverse proxy in a single FQDN deployment on page 150. | |
| 3 | Configure a CA. | See Certificate Authority configuration checklist on page 152.<br>You must have the CA that is used to sign certificates for internal components. | |
| 4 | Enable web socket support. | See Enabling web socket support on page 153. | |

*Table continues…*

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 5 | Configure external and internal traffic rules. | • For configuring external traffic rules, see Configuring external traffic rules in a single FQDN for all services deployment on page 153.<br>• For configuring internal traffic rules, see Configuring internal traffic rules in a single FQDN for all services deployment on page 155. | |

**Related links**

Avaya Session Border Controller for Enterprise configuration checklist on page 147

## Reverse proxy configuration checklist for a multiple FQDN deployment

Perform the tasks outlined in this checklist to configure reverse proxy on the Avaya SBCE if you are using a multiple FQDNs for services.

| No. | Task | Description | ✔ |
|---|---|---|---|
| 1 | Verify prerequisites. | See Prerequisites on page 149. | |
| 2 | Create TLS server profiles for each service in your deployment. | See Checklist for creating TLS server profiles for reverse proxy in a multiple FQDN deployment on page 151. | |
| 3 | Configure a CA | See Certificate Authority configuration checklist on page 152.<br>You must have the CA that is used to sign certificates for internal components. | |
| 4 | Enable web socket support. | See Enabling web socket support on page 153. | |
| 5 | Configure external traffic rules | See Configuring external traffic rules in a multiple FQDN deployment on page 157. | |

**Related links**

Avaya Session Border Controller for Enterprise configuration checklist on page 147

## Prerequisites

Before configuring Avaya SBCE as a reverse proxy:

- Ensure that you have a global FQDN.

- If you are using a single FQDN for all services, ensure that you have the following interfaces on Avaya SBCE:
  - One B1 interface for external traffic.
  - One A1 interface for outgoing HTTP traffic that runs to Avaya Meetings Server Management, Web Collaboration Services, and Avaya Aura® Web Gateway.
  - One A1 interface for internal enterprise HTTP traffic.
- If you are using multiple FQDNs, ensure that you have the following interfaces on Avaya SBCE:
  - One B1 interface per FQDN for each service.
  - One A1 interface for outgoing HTTP traffic that runs to Avaya Meetings Server Management, Web Collaboration Services, and Avaya Aura® Web Gateway components.

## Checklist for creating a TLS server profile for reverse proxy in a single FQDN deployment

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 1 | Create a certificate signing request. | See Certificate setup on page 176.<br>Use the following options specific for this deployment model:<br>• For **Common Name**, use the global FQDN. For example: `webservices.company.com`.<br>• For **Subject Alternative Name**, use the global FQDN. For example: `DNS:webservices.company.com`. | |
| 2 | Download and save the created `.KEY` and `.CSR` files. | | |
| 3 | Send the `.CSR` file to a public CA for signing. | | |
| 4 | Install the signed certificate and the key on the Avaya SBCE. | See Installing a certificate and a key on page 178.<br>When installing the certificate, use a descriptive name. For example: `webservicesCert`. | |

*Table continues…*

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 5 | Create a TLS server profile using the installed certificate. | See Creating a TLS server profile on page 181.<br>When creating a profile, use the certificate installed on the Avaya SBCE in the previous step.<br>Provide a descriptive name for the profile. For example: `webservicesTlsProfile`. | |

**Related links**

Reverse proxy configuration checklist for a single FQDN deployment on page 148

## Checklist for creating TLS server profiles for reverse proxy in a multiple FQDN deployment

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 1 | Create certificate signing requests for each service FQDNs. | See Certificate setup on page 176.<br>Create one certificate for each FQDN used by services deployed in the solution, such as Avaya Meetings Server Management service, Web Collaboration Services, and Avaya Aura® Web Gateway/Portal. If you are using several Web Collaboration Services servers, you need to create a separate CSR for each Web Collaboration Services FQDN. Use the following options specific for this deployment model:<br>• For **Common Name**, use the FQDN assigned to that service. For example: `conferencing_management.company.com` for Avaya Meetings Server Management service.<br>• For **Subject Alternative Name**, use the global FQDN. For example: `DNS:conferencing_management.company.com` for Avaya Meetings Server Management service. | |
| 2 | For each CSR, download and save created `.KEY` and `.CSR` files. | | |

*Table continues…*

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 3 | Send `.CSR` files to a public CA for signing. | | |
| 4 | Install the signed certificates and keys on the Avaya SBCE. | See Installing a certificate and a key on page 178.<br>When installing certificates, use descriptive names. For example: `conferencingManagementCert` for the Avaya Meetings Server Management service certificate.<br>**Note:**<br>When installing a certificate, make sure that you use the corresponding key. Do not install keys of another certificates. | |
| 5 | Create TLS server profiles using the installed certificates. | See Creating a TLS server profile on page 181.<br>When creating profiles, use certificates installed on the Avaya SBCE in the previous step.<br>Provide a descriptive name for each profile. For example: `conferenceMgmtTlsProfile` for the Avaya Meetings Server Management service profile. | |

**Related links**

Reverse proxy configuration checklist for a multiple FQDN deployment on page 149

## Certificate Authority configuration checklist

You must have the CA that is used to sign certificates for internal components.

- In a single FQDN for all services deployment, certificates for internal components are usually signed by the System Manager CA.
- In a multiple FQDN deployment, certificates for internal components are usually signed by a public CA.

To configure a CA, perform the tasks outlined in the following checklist:

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 1 | Install the CA on the Avaya SBCE. | See Installing a CA certificate on Avaya SBCE on page 180.<br>Provide a descriptive name for the CA. For example: `certificateAuthority`. | |
| 2 | Create a TLS client profile. | See Creating a TLS client profile on page 181.<br>When creating the profile, use the CA that you installed in the previous step.<br>Provide a descriptive name for the profile. For example: `certificateAuthorityTlsProfile`. | |

**Related links**

Reverse proxy configuration checklist for a single FQDN deployment on page 148
Reverse proxy configuration checklist for a multiple FQDN deployment on page 149

# Enabling web socket support

### Procedure

1. Log in to the Avaya SBCE web administration portal.
2. Navigate to **Global Profiles** > **Reverse Proxy Policy**.
3. Click **Add**.
4. In the **Rule Name** field, provide a name for the reverse proxy policy and then click **Next**.
5. In the General area, select the **Allow Web Socket** check box.
6. For the other settings, use the default values.
7. Click **Finish**.

# Configuring external traffic rules in a single FQDN for all services deployment

### Before you begin

Ensure that you have:

- The TLS server profile for reverse proxy. For more information, see the TLS server profile creation tasks outlined in Checklist for creating a TLS server profile for reverse proxy in a single FQDN deployment on page 150.

- The TLS client profile for reverse proxy. For more information, see the CA configuration tasks outlined in Certificate Authority configuration checklist on page 152.

Use the same TLS server and client profiles when configuring both external and internal traffic rules.

### Procedure

1. Log in to the Avaya SBCE web administration portal.
2. Navigate to **Device Specific Settings** > **DMZ Services** > **Relay Services** > **Reverse Proxy**.
3. Click **Add**.
4. In **Service Name**, enter a name for the profile.
5. Select the **Enable** check box to enable the reverse proxy profile.
6. In **Listen IP**, select the external B1 interface and the Avaya SBCE external leg IP addresses.
7. In **Listen Port**, enter `443`.
8. In **Listen Protocol**, select **HTTPS**.
9. In **Listen TLS Profile**, select the TLS server profile that you created.

   An example of the TLS profile name is `webservicesTLSProfile`.
10. **Connect IP**: Select the internal A1 interface and the Avaya SBCE internal leg IP address.
11. In **Server Protocol**, select **HTTPS**.
12. In **Server TLS Profile**, select the TLS client profile that you created.

    An example of the TLS client profile name is `certificateAuthorityTLSProfile`.
13. Select the **Rewrite URL** check box.
14. Click **Add** at the bottom of the page to create a set of rules and configure the rules as described in External traffic rules for a single FQDN deployment on page 154.
15. Click **Finish**.

### Related links

External traffic rules for a single FQDN deployment on page 154
Reverse proxy configuration checklist for a single FQDN deployment on page 148

## External traffic rules for a single FQDN deployment

| Server Address | White list URL | URL replace | Description |
|---|---|---|---|
| <Equinox Management FQDN>:443 | `/uwd/rest` | `/uwd/rest` | Equinox Conference Control (UCCS) Avaya Meetings Server Management FQDN resolves to |

*Table continues…*

| Server Address | White list URL | URL replace | Description |
|---|---|---|---|
| <Equinox Management FQDN>:443 | `/uwd/ws` | `/uwd/rest` | the virtual IP of the Avaya Meetings Server Management Server.<br>If you are using a standalone system, this FQDN resolves to the virtual IP address. For example: `conferencing_management.company.com`. |
| <WCS1 FQDN>: 443 | `/wcs1` | `/` | Avaya Aura® Media Server. You must create one entry per each Web Collaboration Services server. The FQDN is the FQDN of each Avaya Aura® Media Server, and it resolves to the corresponding Avaya Aura® Media Server IP. For example: `webconference1.company.com`, `webconference2.company.com`, and so on. |
| <WCS2 FQDN>: 443 | `/wcs2` | `/` | |
| <WCSX FQDN>: 443 | `/wcsX` | `/` | |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 8444 | `/acs` | `/acs` | Avaya Aura® Web Gateway. You must use the FQDN that resolves to the virtual IP address of the Avaya Aura® Web Gateway system. For example: `webgateway.company.com`. |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 8444 | `/ups` | `/ups` | |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 8444 | `/csa` | `/csa` | |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 8444 | `/uwd/dist` | `/uwd/dist` | |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 8444 | `/notification` | `/notification` | |
| <Avaya Aura® Web GatewayVirtual IP FQDN>: 8444 | `/portal` | `/portal` | |

# Configuring internal traffic rules in a single FQDN for all services deployment

## Before you begin

Ensure that you have:

- The TLS server profile for reverse proxy. For more information, see the TLS server profile creation tasks outlined in Checklist for creating a TLS server profile for reverse proxy in a single FQDN deployment on page 150.
- The TLS client profile for reverse proxy. For more information, see the CA configuration tasks outlined in Certificate Authority configuration checklist on page 152.

Use the same TLS server and client profiles when configuring both external and internal traffic rules.

### Procedure

1. Log in to the Avaya SBCE web administration portal.
2. Navigate to **Device Specific Settings** > **DMZ Services** > **Relay Services** > **Reverse Proxy**.
3. Click **Add**.
4. In **Service Name**, enter a name for the profile.
5. Select the **Enable** check box to enable the reverse proxy profile.
6. In **Listen IP**, select the internal A1 interface and the Avaya SBCE external leg IP address.
7. In **Listen Port**, enter `443`.
8. In **Listen Protocol**, select **HTTPS**.
9. In **Listen TLS Profile**, select the TLS server profile that you created.

   An example of the TLS server profile name is `webservicesTlsProfile`.
10. In **Connect IP**, select the internal A1 interface and the Avaya SBCE internal leg IP addresses.
11. In **Server Protocol**, select **HTTPS**.
12. In **Server TLS Profile**, select the TLS client profile that you created.

    An example of the TLS client profile name is `certificateAuthorityTLSProfile`.
13. Select the **Rewrite URL** check box.
14. Click **Add** at the bottom of the page to create a set of rules and configure the rules as described in Internal traffic rules for a single FQDN deployment on page 156.
15. Click **Finish**.

**Related links**

Internal traffic rules for a single FQDN deployment on page 156
Reverse proxy configuration checklist for a single FQDN deployment on page 148

## Internal traffic rules for a single FQDN deployment

| Server Address | White list URL | URL replace | Description |
|---|---|---|---|
| <Equinox Management FQDN>:443 | `/uwd/rest` | `/uwd/rest` | Equinox Conference Control (UCCS) Equinox Management FQDN resolves to the virtual IP of the Equinox Management Server. |

*Table continues…*

| Server Address | White list URL | URL replace | Description |
|---|---|---|---|
| <Equinox Management FQDN>:443 | `/uwd/ws` | `/uwd/rest` | If you are using a standalone system, this FQDN resolves to the virtual IP address. For example: `conferencing_management.company.com`. |
| <WCS1 FQDN>: 443 | `/wcs1` | `/` | Avaya Aura® Media Server. You must create one entry per each Web Collaboration Services server. The FQDN is the FQDN of each Avaya Aura® Media Server, and it resolves to the corresponding Avaya Aura® Media Server IP. For example: `webconference1.company.com`, `webconference2.company.com`, and so on. |
| <WCS2 FQDN>: 443 | `/wcs2` | `/` | |
| <WCSX FQDN>: 443 | `/wcsX` | `/` | |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 443 | `/acs` | `/acs` | Avaya Aura® Web Gateway. You must use the FQDN that resolves to the virtual IP address of the Avaya Aura® Web Gateway system. For example: `webgateway.company.com`. |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 443 | `/ups` | `/ups` | |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 443 | `/csa` | `/csa` | |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 443 | `/uwd/dist` | `/uwd/dist` | |
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 443 | `/notification` | `/notification` | |
| <Avaya Aura® Web GatewayVirtual IP FQDN>: 443 | `/portal` | `/portal` | |

# Configuring external traffic rules in a multiple FQDN deployment

## About this task

Perform this procedure for each service in your deployment. For example, if you have multiple Web Collaboration Services servers in your deployment, you must perform this procedure for each server.

## Before you begin

Ensure that you have:

- TLS server profiles for each service in your deployment. For more information, see the TLS server profile creation tasks outlined in Checklist for creating TLS server profiles for reverse proxy in a multiple FQDN deployment on page 151.

- The TLS client profile for reverse proxy. For more information, see the CA configuration tasks outlined in Reverse proxy configuration checklist for a multiple FQDN deployment on page 149.

### Procedure

1. Log in to the Avaya SBCE web administration portal.
2. Navigate to **Device Specific Settings** > **DMZ Services** > **Relay Services** > **Reverse Proxy**.
3. Click **Add**.
4. In **Service Name**, enter a name for the profile.
5. Select the **Enable** check box to enable the reverse proxy profile.
6. In **Listen IP**, select the external B1 interface and the Avaya SBCE external leg IP address.
7. In **Listen Port**, enter `443`.
8. In **Listen Protocol**, select **HTTPS**.
9. In **Listen TLS Profile**, select the TLS server profile that you created.

   An example of the TLS server profile name for Web Collaboration Services is `webservicesTLSProfile`.
10. In **Connect IP**, select the internal interface A1 and the Avaya SBCE internal leg IP address.
11. In **Server Protocol**, select **HTTPS**.
12. In **Server TLS Profile**, select the TLS client profile that you created.

    An example of the TLS client profile name is `certificateAuthorityTLSProfile`.
13. Select the **Rewrite URL** check box.
14. Click **Add** at the bottom of the page to create a set of rules and configure the rules as described in External traffic rules for a single FQDN deployment on page 154.
15. Click **Finish**.

### Related links

External traffic rules in a multiple FQDN deployment on page 158
Reverse proxy configuration checklist for a multiple FQDN deployment on page 149

## External traffic rules in a multiple FQDN deployment

### Traffic rules for Avaya Meetings Server Management

| Server Address | White list URL | URL replace | Description |
|---|---|---|---|
| <Equinox Management FQDN>:443 | `/uwd/rest` | `/uwd/rest` | Equinox Conference Control (UCCS) Equinox Management FQDN resolves to the virtual IP of the Equinox Management Server. |

*Table continues…*

| Server Address | White list URL | URL replace | Description |
|---|---|---|---|
| <Equinox Management FQDN>:443 | `/uwd/ws` | `/uwd/rest` | If you are using a standalone system, this FQDN resolves to the virtual IP address. For example: `conferencing_management.company.com`. |

### Traffic rules for Web Collaboration Services

| Server Address | White list URL | URL replace | Description |
|---|---|---|---|
| <WCSX FQDN>: 443 | / | / | Avaya Aura® Media Server. You must create one entry per each Web Collaboration Services server. The FQDN is the FQDN of each Avaya Aura® Media Server, and it resolves to the corresponding Avaya Aura® Media Server IP. For example: `webconference1.company.com`, `webconference2.company.com`, and so on. |

### Traffic rules for Avaya Aura® Web Gateway/Portal

| Server Address | White list URL | URL replace | Description |
|---|---|---|---|
| <Avaya Aura® Web Gateway Virtual IP FQDN>: 8444 | / | / | Avaya Aura® Web Gateway. You must use the FQDN that resolves to the virtual IP address of the Avaya Aura® Web Gateway system. For example: `webgateway.company.com`. |

# External client access configuration

The following sections describe how to configure Avaya SBCE if you are planning to use any external clients, including WebRTC, moblile, or desktop clients, outside the enterprise firewall.

## External client access configuration checklist

Perform the tasks outlined in this checklist if you are planning to use any external clients, including WebRTC, mobile, or desktop clients, outside the enterprise firewall.

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 1 | Create a server TLS profile for a management interface. | See Checklist for creation of a TLS server profile for a management interface on page 160. | |

*Table continues…*

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 2 | Configure Avaya SBCE load monitoring. | See Configuring Avaya SBCE load monitoring on page 161. | |
| 3 | Add Avaya SBCE to the Avaya Aura® Web Gateway. | See Adding Avaya Session Border Controller for Enterprise to the Avaya Aura Web Gateway on page 162. | |
| 4 | If you have conferencing, add Avaya SBCE to Avaya Meetings Server Management. | See Adding Avaya Session Border Controller for Enterprise to Avaya Meetings Server Management on page 163. | |
| 5 | Configure WebRTC client side TURN. | See WebRTC client side TURN configuration on page 164. | |
| 6 | Configure support for external native media clients. | See External native clients media configuration on page 168. | |

# Checklist for creation of a TLS server profile for a management interface

Perform the tasks in this checklist to configure certificates and create a TLS server profile for a management interface. This is required for external client access configuration.

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 1 | Create a certificate signing request. | See Creating a certificate signing request on Avaya Session Border Controller for Enterprise on page 176.<br>When creating a CSR, use the following options:<br>• For **Common Name**, use the management interface FQDN. For example: `asbce_management.company.com`.<br>• For **Subject Alternative Name**, provide both the FQDN and IP address of the management interface. For example:<br>`DNS:asbce_management.company.com IP:10.10.10.10`<br>. | |
| 2 | Download and save created `.KEY` and `.CSR` files. | | |

*Table continues…*

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 3 | Send the `.CSR` file to the System Manager CA for signing. | See Signing certificates with the System Manager CA on page 177. | |
| 4 | Install the signed certificate and the key on the Avaya SBCE. | See Installing a certificate and a key on page 178.<br>When installing the certificate, use a descriptive name. For example: `asbceManagementCert`. | |
| 5 | Create a TLS server profile using the installed certificate. | See Creating a TLS server profile on page 181.<br>When creating a profile, use the certificate installed on the Avaya SBCE in the previous step.<br>Provide a descriptive name for the profile. For example: `asbceManagementTlsProfile`. | |

**Related links**

External client access configuration checklist on page 159

# Configuring Avaya SBCE load monitoring

## About this task

Perform this procedure if you are using external clients in your deployment.

## Before you begin

Ensure that you have:

- The internal A1 interface that will be used for load monitoring.

  **Note:**

  This A1 interface must also be used for the TURN relay setup.

- An FQDN for the Avaya SBCE management interface. For more information, see Required FQDNs and certificates on page 29.
- A TLS server profile. For more information about creating this profile, see Checklist for creation of a TLS server profile for a management interface on page 160.

## Procedure

1. Log in to the Avaya SBCE web administration portal.
2. Navigate to **Device Specific Settings** > **Advanced Options** > **Load Monitoring**.
3. Click **Add** to create a new monitoring profile.
4. In **Load Balancer Type**, select **INTERNAL**.

This is the load balancer on the A1 side of the network. Avaya Aura® Web Gateway performs load balancing towards the internal side. All HTTP requests sent for dialing out use the internal load balancer logic to identify the appropriate Avaya SBCE.

5. In **Transport**, select **TLS**.
6. In **TLS Profile**, select the TLS server profile that you created.

   For more information, see the tasks outlined in Checklist for creation of a TLS server profile for a management interface on page 160.
7. In **Listen IP**, select the internal A1 interface.

   To enable external WebRTC clients, the same interface must be configured for the TURN server as the A1 interface.
8. In **Service Type**, select **TURN**.
9. Click **Finish**.

### Next steps

Add Avaya SBCE to the Avaya Aura® Web Gateway.

---

# Adding Avaya Session Border Controller for Enterprise to the Avaya Aura® Web Gateway

### Procedure

1. Log in to the Avaya Aura® Web Gateway web administration portal.
2. Click **Add** to add a new Avaya SBCE or click **Edit** to update the information for the existing Avaya SBCE connection.
3. In **SIP Address**, type the FQDN or IP address of the internal A1 interface of the Avaya SBCE that is used for SIP signaling to interact with Avaya Aura® Web Gateway.

   For more information, see External native clients media configuration on page 168.
4. In **IP Port**, enter `5061`.
5. In **SIP Protocol**, select **TLS**.
6. In **HTTP Address**, type the internal Avaya SBCE FQDN specified for the load monitoring entry.

   For example: `asbce_management.company.com`.
7. In **HTTP Port**, enter `443`.
8. In **HTTP Protocol**, select **https**.
9. In **Location**, specify the location of the Avaya SBCE server.
10. Click **Save**.

### Next steps

If you have conferencing, add Avaya SBCE to Avaya Meetings Server Management.

---

# Adding Avaya Session Border Controller for Enterprise to Avaya Meetings Server Management

### Procedure

1. Log in to the Avaya Meetings Management web administration portal.
2. Navigate to **Devices** > **Devices by Type** > **ASBCE**.
3. Click **Add**.
4. On the Add ABSCE page, do the following:
   a. In **Name**, enter a name for the Avaya SBCE server.
   b. In **IP Address**, enter any of the Avaya SBCE IP addresses.
   c. In **Location**, select the location of the Avaya SBCE server.
5. Click **OK**.
6. Select the Avaya SBCE name from the list and do the following:
   a. In **Listen/Relay Internal IP**, enter the Avaya SBCE IP address of the internal A1 interface configured for the load balancer and for STUN/TURN interface.

      For more information, see Configuring Avaya SBCE load monitoring on page 161 and WebRTC client side TURN configuration on page 164.
   b. In **Port**, enter `3478`.
   c. In **Listen/Relay Public IP**, enter one of the following Avaya SBCE public IP addresses of the STUN/TURN interface:
      - The IP address of the external B1 interface.
      - The firewall NAT public IP address of the external B1 interface.

      For more information about the B1 interface, see WebRTC client side TURN configuration on page 164.
   d. In **Port**, enter `3478`.
   e. In **Internal SIP IP**, type the FQDN or IP address of the internal A1 interface of the Avaya SBCE that is used for SIP signaling.

      For more information about interaction with Avaya Aura® Web Gateway, see External native clients media configuration on page 168.
   f. In **SIP Protocol** select **TLS**.
   g. In **SIP Port**, enter `5061`.

h. In **Local HTTP IP**, enter the internal A1 address configured for the load monitoring entry.

   For example, `asbce_management.company.com`.

i. In **HTTP protocol**, select **https**.

j. In **HTTP port**, enter `443`.

7. Click **OK**.

# WebRTC client side TURN configuration

Avaya recommends using client side TURN instead of sever side TURN whenever possible. If you use server side TURN and WebRTC browsers are behind a firewall that blocks UDP traffic, you might experience issues with WebRTC calls. Clients are loaded from your browser and no installation is required on client users' computers.

Use these sections to enable client side TURN for WebRTC browsers outside your enterprise firewall.

To enable client side TURN, you need to open TCP port 443 on the external firewall.

**Related links**

External client access configuration checklist on page 159

## Checklist for WebRTC client side TURN configuration

Perform the tasks outlined in this checklist to configure external client access.

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 1 | Verify prerequisites. | See Prerequisites on page 165. | |
| 2 | Create a TLS server profile that is used if media tunneling requires better readability through firewalls. | See TLS server profile checklist for client side TURN configuration on page 165. | |
| 3 | Configure firewall rules. | See Firewall configuration on page 166. | |
| 4 | Configure a TURN/STUN profile for WebRTC calls on Avaya SBCE. | See Configuring a TURN/STUN profile for WebRTC calls on Avaya Session Border Controller for Enterprise on page 166. | |
| 5 | Configure the TURN relay service for WebRTC calls on Avaya SBCE. | See Configuring the TURN relay service for WebRTC calls on Avaya Session Border Controller for Enterprise on page 167. | |
| 6 | Configure a STUN server on the Avaya Aura® Web Gateway. | See TURN/STUN service configuration on the Avaya Aura Web Gateway on page 168. | |
| 7 | Enable TURN usage in a WebRTC client. | See Enabling TURN usage in a WebRTC client on page 168. | |

## Prerequisites

Before configuring WebRTC client side TURN settings, do the following:

- Add Avaya SBCE to the Avaya Aura® Web Gateway. For more information, see Adding Avaya Session Border Controller for Enterprise to the Avaya Aura Web Gateway on page 162.
- Configure one B1 interface IP address on the Avaya SBCE.

  Additional internal A1 interfaces are not required. Use the same A1 interface IP that you used for load monitoring. For more information, see Configuring Avaya SBCE load monitoring on page 161.

## TLS server profile checklist for client side TURN configuration

Perform the tasks outlined in this checklist to create a TLS server profile that is used if media tunneling requires better readability through firewalls.

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 1 | Create a certificate signing request. | See Certificate setup on page 176.<br>Use the following options:<br>• For **Common Name**, use the TURN media FQDN. For example: `turnmedia.company.com`.<br>• For **Subject Alternative Name**, use the TURN media FQDN. For example: `DNS:turnmedia.company.com`. | |
| 2 | Download and save the created `.KEY` and `.CSR` files. | | |
| 3 | Send the `.CSR` file to a public CA for signing. | | |
| 4 | Install the signed certificate and the key on the Avaya SBCE. | See Installing a certificate and a key on page 178.<br>When installing the certificate, use a descriptive name. For example: `turnmediaCert`. | |
| 5 | Create a TLS server profile using the installed certificate. | See Creating a TLS server profile on page 181.<br>When creating a profile, use the certificate installed on the Avaya SBCE in the previous step.<br>Provide a descriptive name for the profile. For example: `turnmediaTlsProfile`. | |

# Firewall configuration

## External firewall rules

| Port | Protocol | Decription |
|---|---|---|
| 443 | TLS | For TLS TURN. For traffic that runs from the internet to Avaya SBCE on the B interface.<br>This option is only required if you are using TLS TURN and it provides better readability through firewalls. |
| 3478 | TCP and UDP | For UDP media. For traffic that runs from the internet to Avaya SBCE on the B interface.<br>This option is only required if you are using direct WebRTC media. |

## Internal firewall rules

| Port | Protocol | Desciption |
|---|---|---|
| 3478 | UDP | For UPD media from Avaya SBCE. For traffic that runs from the A interface of Avaya SBCE to the MCU 7K servers and Avaya Aura® Media Server. |
| 50000 to 55000 | UDP | For UPD media from Avaya SBCE. For traffic that runs from the A interface of Avaya SBCE to the MCU 7K servers and Avaya Aura® Media Server. |
| 12000 to 13200 | UDP | For UPD media from media servers. For traffic that runs from MCU 7K servers to the A interface of Avaya SBCE. |
| 16384 to 16984 | UDP | For UPD media from media servers. For traffic that runs from MCU 7K servers to the A interface of Avaya SBCE. |
| 6000 to 32588 | UDP | For UPD media from media servers. For traffic that runs from Avaya Aura® Media Server to the A interface of Avaya SBCE. |

# Configuring a TURN/STUN profile for WebRTC calls on Avaya Session Border Controller for Enterprise

## Procedure

1. Log in to the Avaya SBCE web administration interface.
2. Navigate to **Device Specific Settings** > **TURN/STUN Service**.
3. From the Application pane, select the Avaya SBCE device for which the new TURN/STUN profile will be created.
4. Click **TURN/STUN Profiles**.
5. Click **Add**.

   The system displays the Add TURN/STUN Profile window.
6. In **Profile Name**, provide a name for the TURN/STUN profile.

   For example: `turnProfileForWebrtcCalls`.

7. In **UDP Listen Port**, enter `3478`.
8. In **TCP/TLS Listen Port**, enter `443`.
9. If TLS TURN media is required, then in **TLS Server Profile**, specify the TLS server profile for a management interface that you created.

   For more information, see the tasks outlined in TLS server profile checklist for client side TURN configuration on page 165. An example of the TLS server profile name is `turnmediaTlsProfile`.
10. In **Media Relay Port Range**, specify a range that does not overlap with the port range used by Avaya SBCE for other protocols, such as SIP.

    The default range is 50000 to 55000.
11. Select the **Authentication** check box.
12. Select the **Client Authentication** check box.
13. Select the **UDP Relay** check box.
14. Click **Finish**.

## Configuring the TURN relay service for WebRTC calls on Avaya Session Border Controller for Enterprise

### Procedure

1. Log in to the Avaya SBCE web administration interface.
2. Navigate to **Device Specific Settings** > **TURN/STUN Service**.
3. From the Application pane, select the Avaya SBCE device for which you need to create a new TURN relay service.
4. Click **TURN/STUN Relay**.
5. Click **Add**.

   The system displays the Add TURN/STUN IP Pairing window.
6. In **Listen IP**, provide the listen IP address of the TURN server from the B1 interface.

   **Important:**

   Do *not* use this IP address for any other interface bound to port 443.
7. In **Media Relay**, provide the media relay IP address of the TURN server from the internal A1 interface that you used for load monitoring.
8. In **Service FQDN**, provide the FQDN that resolves to the address specified in the **Listen IP** field.

   For example, `turnmedia.company.com`.
9. In **TURN/STUN Profile**, select the TURN/STUN profile that you created for WebRTC calls.

10. Complete the following fields:

    In **TURN/STUN Profile**, select the TURN/STUN profile that you created for WebRTC calls.

    For example: `turnProfileForWebrtcCalls`. For more information, see Configuring a TURN/STUN profile for WebRTC calls on Avaya Session Border Controller for Enterprise on page 166.

11. Click **Finish**.

## TURN/STUN service configuration on the Avaya Aura® Web Gateway

You can add a new STUN server and set the STUN server priority from **External Access** > **STUN Servers** on the Avaya Aura® Web Gateway administration portal. If you use client side TURN, you must add the IP address of Avaya SBCE as a STUN server. Avaya recommends using client side TURN whenever possible.

You must use port 3478 when adding a new STUN server.

For more information about configuring STUN server settings on Avaya Aura® Web Gateway, see “Managing STUN server settings” in *Administering the Avaya Aura® Web Gateway*.

## Enabling TURN usage in a WebRTC client

### Procedure

1. On the Avaya Aura® Web Gateway administration portal, navigate to **External Access** > **Session Border Controller**.
2. Select the **Enable TURN in WebRTC Client** check box.
3. Click **Save**.

# External native clients media configuration

Use the following sections if you are planning to use Avaya Workplace Client mobile and desktop clients outside of your enterprise firewall.

### Related links

External client access configuration checklist on page 159

## External native clients media configuration checklist

Perform the tasks outlined in this checklist if you are planning to use Avaya Workplace Client mobile and desktop clients outside of your enterprise firewall.

| No. | Task | TLS server profile required for SIP communications with Avaya SBCE | ✔ |
|---|---|---|---|
| 1 | Verify prerequisites. | See Prerequisites on page 169. | |

*Table continues…*

| No. | Task | TLS server profile required for SIP communications with Avaya SBCE | ✔ |
|---|---|---|---|
| 1 | Create a TLS server profile for required for SIP communications with Avaya SBCE. | See TLS server profile checklist for external native clients media configuration on page 169.<br>In a multiple FQDN deployment, you can use the TLS server profile for Avaya Meetings Server Management, which you created during the reverse proxy configuration. For more information, see Checklist for creating TLS server profiles for reverse proxy in a multiple FQDN deployment on page 151. | |
| 2 | Create a TLS server profile for HTTP media tunneling. | See TLS server profile checklist for media tunneling interfaces on page 170. | |
| 3 | Configure firewall rules. | See Firewall configuration on page 171. | |
| 4 | Configure the Avaya SBCE signaling interface. | See Configuring the Avaya Session Border Controller for Enterprise signaling interface on page 172. | |
| 5 | Configure the Avaya SBCE media interface. | See Configuring the Avaya Session Border Controller for Enterprise media interface on page 173. | |
| 6 | Configure Avaya SBCE server flows. | See Configuring Avaya Session Border Controller for Enterprise server flows on page 174. | |

## Prerequisites

Before configuring support for external native clients media, do the following:

- Add Avaya SBCE to the Avaya Aura® Web Gateway. For more information, see Adding Avaya Session Border Controller for Enterprise to the Avaya Aura Web Gateway on page 162.
- Configure one A interface IP address and one B interface IP address on the Avaya SBCE.

## TLS server profile checklist for external native clients media configuration

Perform the following tasks to create a TLS server profile required for SIP communications with Avaya SBCE.

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 1 | Create a certificate signing request. | See Certificate setup on page 176.<br>Use the following options:<br>• For **Common Name**, use the Avaya Meetings Management FQDN. For example: `conferencing_management.company.com`.<br>• For **Subject Alternative Name**, use the Avaya Meetings Management FQDN. For example: `DNS:conferencing_management.company.com`. | |
| 2 | Download and save the created `.KEY` and `.CSR` files. | | |
| 3 | Send the `.CSR` file to the System Manager CA for signing. | See Signing certificates with the System Manager CA on page 177. | |
| 4 | Install the signed certificate and the key on the Avaya SBCE. | See Installing a certificate and a key on page 178.<br>When installing the certificate, use a descriptive name. For example: `conferencingManagementSipCert`. | |
| 5 | Create a TLS server profile using the installed certificate. | See Creating a TLS server profile on page 181.<br>When creating a profile, use the certificate installed on Avaya SBCE in the previous step.<br>Provide a descriptive name for the profile. For example: `conferencingManagementSipTlsProfile`. | |

**Related links**

External native clients media configuration checklist on page 168
TLS server profile checklist for media tunneling interfaces on page 170

## TLS server profile checklist for media tunneling interfaces

Perform the following tasks to create a TLS server profile required for SIP communications with Avaya SBCE.

| No. | Task | Notes | ✔ |
|---|---|---|---|
| 1 | Create a certificate signing request. | See Certificate setup on page 176.<br>Use the following options:<br>• For **Common Name**, use the HTTP media tunneling FQDN. For example: `media.company.com`.<br>• For **Subject Alternative Name**, use the HTTPS media tunneling. For example: `DNS:media.company.com`. | |
| 2 | Download and save the created `.KEY` and `.CSR` files. | | |
| 3 | Send the `.CSR` file to a public CA for signing. | | |
| 4 | Install the signed certificate and the key on the Avaya SBCE. | See Installing a certificate and a key on page 178.<br>When installing the certificate, use a descriptive name. For example: `mediaCert`. | |
| 5 | Create a TLS server profile using the installed certificate. | See Creating a TLS server profile on page 181.<br>When creating a profile, use the certificate installed on Avaya SBCE in the previous step.<br>Provide a descriptive name for the profile. For example: `mediaTlsProfile`. | |

**Related links**

External native clients media configuration checklist on page 168
TLS server profile checklist for external native clients media configuration on page 169

# Firewall configuration

## External firewall rules

| Port | Protocol | Description |
|---|---|---|
| 443 | TCP | For HTTPS media tunneling. From the internet to Avaya SBCE on the B interface.<br>This option is only required if you are using media tunneling and it requires better readability through firewalls. |
| 35000 to 40000 | UDP | For UDP media. From the internet to Avaya SBCE on the B interface.<br>This option is only required if you are using direct RTP media. |

*Table continues…*

| Port | Protocol | Description |
|---|---|---|
| 3400, 3580 | TCP | For UDP media. From the internet to Avaya SBCE on the B interface.<br>This option is only required if you are using direct RTP media. |

### Internal firewall rules

| Port | Protocol | Description |
|---|---|---|
| 35000 to 40000 | UDP | For UDP media from Avaya SBCE. For media traffic that runs from the A interface of Avaya SBCE to the MCU 7K and MCU 6K servers. |
| 12000 to 13200 | UDP | For UDP media from media services. For media traffic that runs from MCU 7K servers to the A interface of Avaya SBCE. |
| 16384 to 16984 | UDP | For UDP media from media services. For media traffic that runs from MCU 7K servers to the A interface of Avaya SBCE. |
| 6000 to 17999 | UDP | For UDP media from media services. For media traffic that runs from Avaya Aura® Media Server to the A interface of Avaya SBCE. |
| 5061 | TCP | For SIP communications. For traffic that runs from the Avaya Aura® Web Gateway to the Avaya SBCE SIP communications A interface. |
| 5061 | TCP | For SIP communications. For traffic that runs from the Avaya SBCE SIP communications A interface to the Avaya Meetings Management server. |

## Configuring the Avaya Session Border Controller for Enterprise signaling interface

### About this task

Use this procedure to configure a signaling interface that will be used for SIP communication between the Avaya Aura® Web Gateway and Avaya SBCE.

### Procedure

1. Log in to the Avaya SBCE web administration portal.
2. Navigate to **Device Specific Settings** > **Signaling Interface**.
3. Click **OK**.
4. In **Name**, provide a name.
5. In **IP Address**, provide the network name, identified by the interface name and VLAN tag, and IP address of the Avaya SBCE used by SIP signaling messages traversing the network.
6. Leave the **TCP Port** field blank.
7. Leave the **UDP Port** field blank.

8. In **TLS Port**, enter `5061`.
9. In **TLS Profile**, select the TLS server profile created for SIP signaling.

   For example: `conferencingManagementSipTlsProfile`. For more information, see TLS server profile checklist for external native clients media configuration on page 169.
10. Click **Finish**.

## Configuring the Avaya Session Border Controller for Enterprise media interface

### About this task

Media data can be passed through the default UDP port range or tunneled through port 443.

### Procedure

1. Log in to the Avaya SBCE web administration portal.

Perform steps 2 and 3 if you want to set up media data tunneling through port 443. Otherwise, continue from step 4.

2. Navigate to **Device Specific Settings** > **Advanced Options** > **Feature Control**.
3. Select the **Media Tunneling** check box and then click **Save**.
4. To configure an external media interface, do the following:
   a. Navigate to **Device Specific Settings** > **Media Interface** and then click **Add**.
   b. In **Name**, provide a name for the media interface.

      For example: `externalMediaInterfaceProfile`.
   c. From **IP Address**, select the B1 IP address.

      **Important:**

      - Do not use this IP address for any other interface bound to port 443, such as for HTTP tunneling configuration.
      - Do not use VLAN tag for the media tunneled interface.
   d. If you are using media tunneling, from **TLS Profile**, select the required TLS server profile for the media interface that you have created when performing TLS server profile checklist for media tunneling interfaces on page 170.

      For example, `mediaTlsProfile`.

      If media tunneling is disabled, set this field to **None**.
   e. In **Buffer Size**, provide the required buffer size for media data.
5. To configure the internal media interface, do the following:
   a. Navigate to **Device Specific Settings** > **Media Interface** and then click **Add**.
   b. In **Name**, provide a name for the media interface.

      For example: `internalMediaInterfaceProfile`.

c. From **IP Address**, select the A1 IP address.

6. To enable video media, do the following:
   a. Navigate to **Domain Policies** > **Application Rules** and then clone an existing media rule or create a new one.
   b. For the new application rule, select **In** and **Out** for both the Audio and Video application types.
   c. Configure **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** as required.
   d. Click **Finish**.
7. To configure media encryption and enable Binary Floor Control Protocol (BFCP) or Far End Camera Control (FECC), do the following:
   a. Navigate to **Domain Policies** > **Media Rules** and clone an existing media rule or create a new one.
   b. For the new media rule, navigate to **Encryption** > **Miscellaneous** and select the **Capacity Negotiation** check box.
   c. On the Audio Encryption screen, in all **Preferred Format** fields, select **SRTP_AES_CM_128_HMAC_SHA1_80**.
   d. On the Advanced tab, select the **BFCP Enabled** and **FECC Enabled** check boxes.
8. To configure a policy group using the newly created application and media rules, navigate to **Domain policies** > **End Point Policy Groups** , create a new group, and add the required application and media rules to that group.

## Configuring Avaya Session Border Controller for Enterprise server flows

### Before you begin

Ensure that you have the TLS client profile created when you configured a certificate authority for reverse proxy. For more information, see Certificate Authority configuration checklist on page 152. An example of the TLS client profile name is `certficateAuthorityTlsProfile`.

### Procedure

1. Log in to the Avaya SBCE web administration portal.
2. To create an interworking profile, do the following:
   a. Navigate to **Global Profiles** > **Server Interworking** and then select **Add**.
   b. For the new profile, use the default options for all settings.
   c. In the Advanced Options section, set **Has Remote SBC** to **No (disabled)**.
3. To add a configuration for Avaya Meetings Management, do the following:
   a. Navigate to **Global Profiles** > **Server Configuration** and then click **Add**.
   b. From **Sever Type**, select **Trunk Server**.

c. Leave **SIP domain** blank.

d. From **TLS Client Profile**, select the TLS client profile that you created when you configured a certificate authority for reverse proxy.

e. Add the Avaya Meetings Management FQDN with port 5061 and the TLS protocol specified.

f. In the Advanced Options section, select the **Enable Grooming** check box and then select the previously created interworking profile.

4. To add a configuration for the Avaya Aura® Web Gateway, do the following:

a. Navigate to **Global Profiles** > **Server Configuration** and then click **Add**.

b. From **Sever Type**, select **Trunk Server**.

c. Leave **SIP domain** blank.

d. From **TLS Client Profile**, select the TLS client profile that you created when you configured a certificate authority for reverse proxy.

e. Add the Avaya Aura® Web Gateway FQDN with port 5061 and TLS protocol specified.

f. Repeat the previous substep for FQDNs of all Avaya Aura® Web Gateway nodes.

g. In the Advanced Options section, select the **Enable Grooming** check box and then select the interworking profile created in the previous step.

5. To add a flow for Avaya Meetings Management, do the following:

a. Navigate to **Device Specific Settings** > **End Point Flows** > **Server Flows** and then select **Add**.

b. In **Flow Name**, provide a name for the flow.

For example: `EqMngFlow`.

c. From **Server Configuration**, select the Avaya Meetings Management configuration that you created in step 3.

d. From **Received Interface**, select the internal A1 interface.

e. From **Signaling Interface**, select the internal A1 interface.

f. From **Media Interface**, select the internal A1 interface.

g. From **End Point Policy Group**, select **required**.

6. To add a flow for the Avaya Aura® Web Gateway, do the following:

a. Navigate to **Device Specific Settings** > **End Point Flows** > **Server Flows** and then select **Add**.

b. In **Flow Name**, provide a name for the flow.

For example: `AAWGFlow`.

c. From **Server Configuration**, select the Avaya Aura® Web Gateway configuration that you created in step 4.

d. From **Received Interface**, select the internal A1 interface.
e. From **Signaling Interface**, select the internal A1 interface.
f. From **Media Interface**, select the external B1 interface.
g. From **End Point Policy Group**, select **required**.

# Certificate setup

The following sections describe how to configure certificates. Use the web administration interface to configure System Manager certificates. The configuration utility (app configure) only supports third party certificates.

## Creating a certificate signing request on Avaya Session Border Controller for Enterprise

### Procedure

1. Log in to the Avaya SBCE web administration interface.
2. Navigate to **TLS Management** > **Certificates**.
3. Click **Generate CSR**.
4. Complete the following fields:
   a. **Country Name**: Provide the name of the country within which the certificate is being created in the ISO 3166 format.
   b. **State/Province Name**: Provide the state or province where the certificate is being created.
   c. **Locality Name**: Provide the city where the certificate is being created.
   d. **Organization Name**: Provide the name of the company or organization creating the certificate.
   e. **Organizational Unit**: Provide the group within the company or organization creating the certificate.
   f. **Common Name**: Provide a FQDN that resolves to the IP address of the server where this certificate will be installed. You cannot provide wildcard (*) characters in the field.
   g. **Algorithm**: Select **SHA256**.
   h. **Key Size (Modulus Length)**: Select **2048**.
   i. **Key Usage Extension(s)**: Select the purpose for which the public key might be used: Key Encipherment, Non-Repudiation, or Digital Signature.
   j. **Extended Key Usage**: Select **Server Authentication** and **Client Authentication**.

k. **Subject Alt Name**: Provide information FQDNs or IP addresses that must be included into the certificate.

   Use the following format: `DNS:<FQDN>,IP:<IP address>`.

   You can specify multiple FQDNs or IP addresses.

l. **Passphrase**: Proivde the password used when encrypting the private key.

m. **Confirm Passphrase**: Reenter the password that you entered in the **Passphrase** field.

n. **Contact Name**: Provide the name of the individual within the issuing organization acting as the point-of-contact for issues relating to this certificate.

o. **Contact E-mail**: Provide the email address of the contact.

5. Click **Generate CSR**.
6. Download and save the CSR request file in the `.CSR` format.
7. Delete the key file generated and saved on Avaya Session Border Controller for Enterprise.

### Next steps

Provide the `.CSR` file to a CA for signing.

## Signing certificates with the System Manager CA

### Procedure

1. Log in to the System Manager web administration portal.
2. Navigate to **Security** > **Certificates** > **Authority**.
3. Ensure that the certificate profile is set as follows:
   a. **Key Usage Extension** set to Digital Signature and Key Encipherment.
   b. **Extended Key Usage**: set to Server Authentication and Client Authentication.
4. If you do not have an end entity, do the following:
   a. Navigate to **Add End Entity**.
   b. Provide a user name and password for the new entity.

      The user name and password are required for issuing the certificate.

   c. Continue performing the procedure from step 6.
5. If you already configured an end entity, do the following:
   a. Navigate to **Search End Entity**.
   b. Enter the user name that you provided when creating the entity and then click **Edit End Entity**.

c. In **Status**, select **New** and enter the password.

d. Continue performing the procedure from the following step.

6. Configure the end entity fields as follows:

   a. **Subject DN > CN**: FQDN of the server interface that provides TLS support.

   b. **Subject Alternative Name**: For **DNS name**, enter the FQDN of the server interface that provides TLS support, and for **IP Address**, enter the UP address of the IP requiring TLS support.

   c. **Certificate Profile**: Enter `ID_CLIENT_SERVER` with relevant key features.

   d. **CA**: Enter `tmdefaultca`.

   e. **Token**: Select **User Generated**.

7. Click **Add** if you are configuring a new entity or **Save** if you are configuring the existing entity.
8. Navigate to **Public Web** > **Enroll**.
9. Click **Create Certificate from CSR**.
10. Enter the user name and password that you used when creating the end entity.
11. Open the CSR request file in the `CSR` format in a text editor and copy its content into a text box on the page.
12. In **Result Type**, select **PEM certificate only**.
13. Click **OK**.

    A certificate file in the `.PEM` format is created.

14. Save the certificate file on an external storage device.

### Next steps

Install the signed certificate.

---

# Installing a certificate and a key

### Procedure

1. Rename the certificate key in the `.PEM` format and the key file in the `.KEY` format so that these files use the same file name.

   For example: `certificate1.pem` and `certificate1.key`.

   **Important:**

   Do not use the dot (.) symbol in the file name.

2. Log in to the Avaya SBCE web administration portal.
3. Navigate to **TLS Management** > **Certificates**.

4. Click **Install**.
5. Configure the following fields:
   a. **Type**: Select a type of the certificate that you want to install.
   b. **Name**: Provide a name for the certificate that you want to install.

      This field is optional. If you do not provide a name, then the file name of the uploaded certificate file will be used as the certificate name.

      **Note:**

      If you provide a name that matches the name of one of installed certificates, the system replaces that certificate with the certificate that you are installing.

   c. **Override Existing**: Select if you can install a certificate with the name that matches the name of one of already installed certificates.

      If the check box is cleared, the system displays an error message when you try to install a certificate with the same name. If the check box is selected, the system replaces the existing certificate with the certificate you are installing.

   d. **Allow Weak Certificate Key**: Select if you can install a certificate signed using a weak key.

      If the option is selected, the system bypasses the check that requires strong private keys. EMS rejects private keys lesser than 2048 bits or signed with an MD5 based hash by default.

   e. **Certificate File**: Specify a location of the certificate file on your computer.

      **Important:**

      If the third-party CA provides separate Root CA and intermediate certificates, you must combine these certificates into a single file before installing to Avaya SBCE. To combine the files, append the content of each certificate file one after another. Add the content of the root CA certificate to the end of this single file.

   f. **Key**: Specify the private key that you want to use.

      You can opt to use the existing key from the file system or select a file containing another key.

   g. **Key File**: Specify the key file.

      This button is displayed when you select **Upload Key File** in the **Key** field.
6. Click **Upload**.
7. Log in to Avaya SBCE as root using an SSH connection.

   The port is 222. Use the ipcs user name and password.
8. Navigate to the `/usr/local/ipcs/cert/key` directory.
9. Run the `enc_key <filename> <passphrase>` command.

In this command, `<filename>` is the name of the encryption key file and `<passphrase>` is the passphrase you used while generating the CSR.

10. Restart Avaya SBCE.

## Installing the Avaya Meetings Management CA certificate to Avaya SBCE

### Procedure

1. Log in to the Avaya Meetings Management web administration portal.
2. Navigate to **Settings** > **Security** > **Certificates**.
3. Click on the Avaya Meetings Management certificate and download the `caroot.crt` file.
4. Log in to the Avaya SBCE web administration portal.
5. Navigate to **TLS Management** > **Certificates**.
6. Click **Install**.
7. Configure the following fields:
   a. **Type**: Select **CA Certificate**.
   b. **Name**: Enter a name for the certificate.
   c. **Overwrite Existing**: Select if you want to overwrite an existing certificate with the name that matches the name of the certificate you are installing.
   d. **Allow weak Certificate key**: Select this check box if the CA certificate is signed with a week key.
   e. **Certificate File**: Select the `caroot.crt` certificate downloaded from the Avaya Meetings Management web administration portal.
8. Click **Upload**.

## Installing a CA certificate on Avaya SBCE

### Procedure

1. Log in to the System Manager web administration portal.
2. Navigate to **Security** > **Certificates** > **Authority** > **CA Structure & CRLs**.
3. Download the required CA certificate file in the `.PEM` format.
4. Log in to the Avaya SBCE web administration portal.
5. Navigate to **TLS Management** > **Certificates**.
6. Select **Install**.

7. Complete the following fields:
   a. **Type**: Select **CA Certificate**.
   b. **Name**: Enter a name for the certificate.

      If you have not downloaded the Private Key, you must type the name you provided in the **Common Name** field while generating CSR. If you have downloaded the Private Key, you can type any name for the certificate.
   c. **Overwrite Existing**: Select if you need to replace the existing certificate that has the same name.
   d. **Allow Weak Certificate Key**: Select if the certificate is signed with a weak key.
   e. **Certificate File**: select the CA certificate file downloaded from Avaya Meetings Management.
8. Press **Upload**.

# TLS client and server profiles setup

## Creating a TLS server profile

### Procedure

1. Log in to the Avaya SBCE web administration portal.
2. Navigate to **TLS Management** > **Server Profiles**.
3. Click **Add**.
4. In **Profile Name**, enter a name for the profile.
5. In **Certificate**, select the installed CA certificate that you want to associate with the profile.
6. If you are creating a profile for media tunneling interfaces, in the **Peer Verification** field, select **Optional**.
7. Complete the remaining fields as required and then click **Next**.
8. Select the required TLS versions and then click **Finish**.

   The system displays the new profile on the Server Profile page.

## Creating a TLS client profile

### Procedure

1. Log in to the Avaya SBCE web administration portal.

2. Navigate to **TLS Management** > **Client Profiles**.
3. Click **Add**.
4. In **Profile Name**, enter a name for the profile.
5. In **Certificate**, select the installed CA certificate that you want to associate with the profile.
6. Complete the remaining fields as required and then click **Next**.
7. Select the required TLS versions and then click **Finish**.

   The system displays the new profile on the Client Profile page.

# Configuring Avaya SBCE network interfaces

### Procedure

1. Log in to the Avaya SBCE web administration portal.
2. Navigate to **Device Specific Settings** > **Network Management** > **Networks**.
3. Configure the following interfaces:
   - Internal interface A1 with at least one IP address associated with it.
   - External interface B1 with at least one IP address associated with it.

# Chapter 10: Resources

## Documentation

The following table lists other related documentation. All Avaya documentation is available at http://support.avaya.com/. Many documents are also available at http://documentation.avaya.com/.

| Title | Use this document to: | Audience |
|---|---|---|
| Overview and planning | | |
| *Avaya Aura® Core Solution Description* | Understand the strategic, enterprise, and functional views of the Avaya Aura® architecture. | • Customers<br>• Sales, services, and support personnel |
| *Avaya Aura® Communication Manager Feature Description and Implementation* | Understand the features of Avaya Aura® Communication Manager. | |
| *What's New in Avaya Aura® Release 8.1.x* | Understand the new and enhanced features of Avaya Aura® components. | • Contractors<br>• Employees<br>• Channel associates<br>• Sales, services, and support personnel<br>• Avaya Business Partners |
| Using | | |
| *Avaya Scopia® Desktop Client User Guide* | Use the Avaya Scopia® desktop client. This document also provides usage information for the user portal. | End users |
| Deploying | | |
| *Deploying Avaya Aura® Device Services* | Install, administer, configure, and maintain Avaya Aura® Device Services. | Implementation personnel |
| *Deploying Avaya Multimedia Messaging* | Install, configure, and administer Avaya Multimedia Messaging. | |

*Table continues…*

| Title | Use this document to: | Audience |
|---|---|---|
| *Deploying Avaya Meetings Server* | Install, configure, and maintain the Avaya Meetings Server. | |
| Administering | | |
| *Administering Avaya Aura® Device Services* | Use management tools, manage data and security, and perform periodic maintenance tasks in Avaya Aura® Device Services. | • System administrators<br>• Implementation personnel<br>• Services and support personnel |
| *Administering Avaya Aura® Communication Manager* | Administer Avaya Aura® Communication Manager on the following servers:<br>• Avaya media gateways<br>• Avaya S8XXX Servers | |
| *Administering Network Connectivity on Avaya Aura® Communication Manager* | Understand the network components of Avaya Aura® Communication Manager. | |
| *Administering Avaya Aura® Session Manager* | Administer Avaya Aura® Session Manager. | |
| *Administering Avaya Aura® System Manager* | Perform configuration and management tasks in Avaya Aura® System Manager. | |
| *Administering Avaya Session Border Controller for Enterprise* | Perform configuration, system administration, and troubleshooting tasks in Avaya Aura® Session Border Controller. | |
| *Implementing and Administering Avaya Aura® Media Server* | Perform configuration, system administration, and troubleshooting tasks in Avaya Aura® Media Server. | |

# Finding documents on the Avaya Support website

## Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.

7. Click **Enter**.

## Avaya Documentation Center navigation

The latest customer documentation for some programs is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

**Important:**

For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for content by doing one of the following:
  - Click **Filters** to select a product and then type key words in **Search**.
  - From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** ( ).

  Navigate to the **Manage Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add topics from various documents to a collection.
  - Save a PDF of selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collection that others have shared with you.
- Add yourself as a watcher using the **Watch** icon ( ).

  Navigate to the **Manage Content** > **Watchlist** menu, and do the following:
  - Enable **Include in email notification** to receive email alerts.
  - Unwatch selected content, all content in a document, or all content on the Watch list page.

  As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.
- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

**Note:**

Some functionality is only available when you log on to the website. The available functionality depends on the role with which you are logged in.

# Training

Avaya Workplace Client solution courses and credentials, such as ACCS-7240, also include information about Avaya Aura® Web Gateway. You can access training courses at http://www.avaya-learning.com.

# Viewing Avaya Mentor videos

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

### About this task

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

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

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

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

  **Note:**

  Videos are not available for all products.

# Support

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

## Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

# Appendix A: Certificate configuration using the configuration utility

The following sections describe how to configure certificates using the configuration utility process. You can only use the configuration utility for the configuration of third party certificates. If you are using System Manager certificates, you must use the web administration portal.

You can also manage and update certificates using the Avaya Aura® Web Gateway web administration portal. For more information about working with the web administration portal, see *Administering the Avaya Aura® Web Gateway*.

**Important:**

The web administration portal is the preferred method for managing certificates. Use the configuration utility process to configure certificates for troubleshooting purposes, but after this is done, perform certificate management from the web administration portal when possible.

## Generating Certificate Signing Requests

### About this task

Use this procedure to generate a Certificate Signing Request (CSR).

**Important:**

You must use this procedure if you are not using System Manager as the only Certificate Authority (CA) to sign certificates for all solution components.

### Before you begin

Ensure that Avaya Aura® Web Gateway is successfully installed with System Manager signed certificates. This is the default setting for installation.

### Procedure

1. Run the following command:

```
sudo mkdir /opt/Avaya/AAWGportalCerts
sudo chmod 770 /opt/Avaya/AAWGportalCerts
```

The system creates an `AAWGportalCerts` directory in `/opt/Avaya/` for the output of the script that will generate the CSRs.

2. Run the following command to navigate to the directory containing the script:

```
cdto misc
```

3. To generate a CSR, run the following command:

```
sudo ./createCSR.sh /opt/Avaya/AAWGportalCerts frontEndFQDN localFQDN
organizationNameorganizationUnit locality stateOrProvince countryCode emailAddress
```

**Important:**

This command is a single Linux command and must be entered as a single line even if it appears as several lines in the document.

The parameters for this script are:

- `frontendFQDN`: For a cluster installation, this is the FQDN of the Virtual IP or external load balancer. For simple, non-clustered installations, this is the FQDN of the server where Avaya Aura® Web Gateway is installed.
- `localFQDN`: The FQDN of the server.
- `orgnizationName`: The name of the organization.
- `organizationUnit`: The name of the unit or sub-organization. For example, “Design”.
- `locality`: The name of the city or town.
- `state`: The two-digit state or province code.
- `countryCode`: The two-digit country code.
- `emailAddress`: The administrator email address.

4. Verify that `/opt/Avaya/AAWGportalCerts` contains the `.key` and `.csr` files for front-end, node, OAMP, and SIP.

   Only the `frontEnd.csr` and `frontEnd.key` files are used. You can ignore the `sip`, `oamp & node .csr` and `.key` files.

# Getting certificates signed by the third-party CA

## About this task

Avaya Aura® Web Gateway accepts certificates in either the PEM or PKCS12 formats.

**Note:**

- PEM is a Base64 encoded ASCII format. The certificate data is prefixed with the `-----BEGIN CERTIFICATE-----` line and followed by the `-----END CERTIFICATE-----` line. The most common file name extensions are `.pem`, `crt`, and `cer`.

- PKCS12 is a binary format that contains the server certificate, intermediate certificates and the private key in a single encryptable file. The file name extensions for this format are `.pfx` and `.p12`.

### Before you begin

- Ensure that the CA is configured to include extendedKeyUsage for both the client and the server in the generated certificates.
- Open the Linux shell using the Linux administrator account credentials.

### Procedure

1. Transfer the `frontEnd.csr` file from Avaya Aura® Web Gateway so that it can be used during signed certificate generation process on your third-party CA.
2. Transfer certificates to Avaya Aura® Web Gateway.
   a. Transfer the signed `.crt` file to `/opt/Avaya/AAWGportalCerts`, and name it `frontEnd.crt`.
   b. Transfer the third-party root CA certificate to `/opt/Avaya/AAWGportalCerts`, and name it `rootCA.crt`.
   c. Transfer any third-party intermediary CA certificates to `/opt/Avaya/AAWGportalCerts`, and name them `intermediary1.crt`, `intermediary2.crt`, and so on in ascending order of the certificate chain until the root CA.
3. To create a certificate chain containing the front end certificate, arrange all intermediary CA certificates (if any) and the root CA certificate in the correct order, and then run the following command:

```
cat frontEnd.crt intermediary1.crt intermediary2.crt ... rootCA.crt >
frontEndCerts.crt
```

# Applying third-party signed certificates to the Avaya Aura® Web Gateway

### Procedure

1. Open the Linux shell using your Linux administrator account credentials.

   The Linux administrator account is created during the deployment process.
2. To open the Avaya Aura® Web Gateway configuration utility, run the following command:

```
app configure
```

3. Select **Front-end host, System Manager and Certificate Configuration**.
4. Select **Use System Manager for Certificates**, and then select **No**.

5. Select the following options, type the file path shown, and then select **OK** for each option:
   a. For **REST interface key file**, type `/opt/Avaya/AAWGportalCerts/frontEnd.key`.
   b. For **REST interface certificate file**, type `value /opt/Avaya/AAWGportalCerts/frontEndCerts.crt`.
   c. For **OAM interface key file**, type `value /opt/Avaya/AAWGportalCerts/frontEnd.key`.
   d. For **OAM interface certificate file**, type `value /opt/Avaya/AAWGportalCerts/frontEndCerts.crt`.
   e. For **Keystore password**, type the same keystore password that you used at the time of installation.
6. Select **Apply** and **Continue** for the specified certificates to be processed.
7. Select **Exit Configure** to exit this menu.

# Adding third-party root CA certificates to the Avaya Aura® Web Gateway

### About this task

Use this procedure to trust additional root CAs. For example, you can add the:

- LDAP root CA certificate if you are using a secure LDAP connection.
- SIP CA certificate if Session Manager has certificates signed by the SIP CA.

You can manage truststore certificates by using the Avaya Aura® Web Gateway administration portal as described in *Administering the Avaya Aura® Web Gateway*.

Do not use this procedure to add the System Manager root CA certificate because that was already added during the initial installation.

### Procedure

1. Run the following command to open the configuration utility:

   ```
   app configure
   ```

2. Select **Add a Certificate to the TrustStore**.
3. To add a certificate, select **Certificate file** and specify the path to the file.
4. Select **Apply**.

   If the provided file contains certificate chain, then all certificates will be added to the truststore.

# Creating a Certificate Signing Request (CSR) using OpenSSL

### About this task

Use this procedure to generate a CSR using OpenSSL.

You can also generate a CSR using the Avaya Aura® Web Gateway web administration portal.

### Before you begin

Ensure that you have the OpenSSL utility.

### Procedure

1. Create an OpenSSL configuration file.

   For example:

   ```
   [ req ]
   req_extensions = v3_req
   distinguished_name = req_distinguished_name

   [req_distinguished_name]

   [ v3_req ]
   basicConstraints = CA:FALSE
   keyUsage = nonRepudiation, digitalSignature, keyEncipherment
   subjectAltName = @alt_names

   [alt_names]
   DNS.1 = dnsserver10927.company.com
   DNS.2 = dnsserver10938.company.com
   DNS.3 = dnsserver10955.company.com
   ```

   The `alt_names` section defines the Subject Alternative Names list and must contain FQDNs of all nodes in the cluster.

2. Run the following command:

   ```
   openssl req -out <CSR_request_file>.csr -newkey rsa:2048 -nodes -keyout
   <CSR_key_file>.key -config <configuration_file>
   ```

   In this command:

   - `<CSR_request_file>.csr` specifies a CSR file name.
   - `<CSR_key_file>.key` specifies a file containing a private key that is used to add the signed certificate to the system.
   - `<configuration_file>` specifies the OpenSSL configuration file that was created in the previous step.

   For example:

   ```
   openssl req -out createCSR.csr -newkey rsa:2048 -nodes -keyout keyCSR.key -config
   configCSR.config
   ```

# Signing identity certificates for Avaya Aura® Web Gateway using third-party CA certificates

## About this task

You can use the following procedure to sign identity certificates for Avaya Aura® Web Gateway using third-party CA certificates.

**Note:**

In the following procedure, the third-party CA certificate can be a public CA or an internal private CA.

## Before you begin

- Create a CSR with the following X509 extensions:
  - keyUsage = nonRepudiation, digitalSignature, keyEncipherment
  - extendedKeyUsage = serverAuth, clientAuth
- Ensure that the CSR contains the following:
  - If the certificate is only used on the Avaya SBCE, the request contains the subjectAltName extension that lists the cluster FQDN in the SAN.
  - If the certificate is used on both Avaya SBCE and the Avaya Aura® Web Gateway server, the request contains the subjectAltName extension that lists the cluster FQDN as well as the FQDN of each cluster member in the SAN.

    **Note:**

    From the security perspective, Avaya recommends that you generate separate certificates for each node, including the cluster FQDN and the individual cluster node FQDN in subjectAltName.
- Do *not* provide the password for a key because password protected keys are not supported.
- Ensure that the key generated along with the CSR is stored safely.
- Ensure that once the certificate is generated, you have received the identity certificate, root CA certificate, and all intermediate CA certificates in the `.PEM` format from the certification authority. If these certificates are not in the `.PEM` format, you can convert these certificates using the OpenSSL tool.
- Generate the identity certificate chain as described in Generating an identity certificate chain on page 194.
- Obtain the System Manager root CA certificate.

## Procedure

1. Log on to Avaya Aura® Web Gateway using your SSH credentials.
2. Go to `/opt/Avaya/CallSignallingAgent/version/CAS/version/nginx/certs`.
3. Run the following command:

```
sudo cat rootCA.pem >> auth_ca.crt
```

In this command, `>>` is used to append the root CA certificate file to the end of the `auth_ca.crt` file.

4. Check that each certificate in the `auth_ca.crt` file is correct using the OpenSSL command.

   You should see the new root CA certificate and the System Manager root CA certificate.

5. Import the intermediate CA certificate and the root CA certificate to the Avaya SBCE trust store if you are using reverse proxy on the Avaya SBCE to Avaya Aura® Web Gateway.
6. Run the Avaya Aura® Web Gateway configuration utility using the `app configure` command.
7. Click **Front-end host, System Manager and Certificate Configuration**.
8. Click **Use System Manager for Certificates** and type `n` to not use System Manager for certificates.
9. Click **REST Interface certificate configuration**. If the certificate is not in the PKCS12 format, type `n` on the REST Interface certificate configuration screen.
10. Add the key file to the REST interface PEM key file and the certificate chain to the REST interface PEM certificate file.
11. Click **Signing authority certificate configuration** on the Front-end host, System Manager and Certificate Configuration screen.
12. If the CA root certificate is not in the PKCS12 format, type `n`.
13. Click **Signing Authority PEM certificate file** and add the signing authority CA certificate.
14. Click **Return to previous menu**.
15. Click **Apply**.

# Generating an identity certificate chain

## About this task

If you want to use an identity certificate signed by a third-party certificate authority (CA), you must generate an identity certificate chain. An identity certificate chain must include the following certificates in order:

1. The third-party CA-signed identity certificate.
2. All intermediate CA certificates, if any.
3. The root CA certificate.

Assign this certificate chain to a specific Avaya Aura® Web Gateway server interface.

## Before you begin

Upload the third-party CA-signed identity certificate, root CA certificate, and all intermediate CA certificates in the PEM format to Avaya Aura® Web Gateway using a file transfer program, such as SFTP or SCP.

### Procedure

1. Log in to the Avaya Aura® Web Gateway using your SSH credentials.
2. Navigate to the directory with the certificates.
3. Run the **cat** command as follows:

   ```
   cat <Identity_ertificate_file_name>
   <Intermediate_CA_certificate_file_name> <Root_CA_file_name> >
   <Certificate_chain_file_name>
   ```

   If you have several intermediate CA certificates, list all intermediate CA certificate file names, separated by a space, and then list the root CA certificate file name.

   For example, if you have the identity certificate `identity.crt`, two intermediate CA certificates (`intermediateCA1.crt` and `intermediateCA2.crt`), and root CA certificate `rootCA.crt`, run the following command to generate a certificate chain with the `identityChain.crt` file name:

   ```
   cat identity.crt intermediateCA1.crt intermediateCA2.crt rootCA.crt
   > identityChain.crt
   ```

# Configuring System Manager to trust third-party root CA certificates

### Procedure

1. Log on to the System Manager web console.
2. Click **Home** > **Services** > **Inventory** > **Manage Elements** .
3. Select System Manager from the **Elements**.
4. Click **Configure Trusted Certificates** in the **More Actions** list.
5. Click **Add** and select **Import from file**.
6. Click **Choose File** and browse to the third-party root CA certificate.
7. Click **Commit**.
8. Restart the System Manager JBOSS™ process.

   From the SSH session on the System Manager, run the following command as a root user:

   ```
   service jboss restart
   ```

   **Note:**

   The **service jboss restart** command affects the service for the System Manager.

# Creating a client certificate

## About this task

Use this procedure to create a client certificate, which can be imported into a web browser for authenticating automatic login into the Avaya Aura® Web Gateway web administration portal.

## Procedure

1. Open the Linux shell using your Linux administrator account credentials.
2. Run the following command to create the `oamp.csr` and `oamp.key` files:

   ```
   sudo /opt/Avaya/CallSignallingAgent/<version>/CAS/<version>/misc/createCSR.sh
   ```

3. To generate the `.pem` file, on the System Manager web console, navigate to **Services** > **Security** > **Certificates** > **Authority**.
4. Click the **Add End Entity** tab and complete the following settings:
   a. Set **End Entity Profile** to **Empty**.
   b. Type your user name and password in **Username** and **Password**.
   c. Type your user ID in **CN, Common name**.

      The user ID you provide must use the same format that you used for the **UID Attribute ID** field on the LDAP Configuration tab.

   d. Set **Certificate Profile** to **ENDUSER**.
   e. Click **Add**.

      A new end entity with the specified user name is created on the System Manager web console.
5. In the left navigation pane, click the **Public Web** tab and complete the following settings:
   a. In **Username** and **Enrollment code** , type the same user name and password that you used to create an end entity.
   b. Click **Choose File** to add the `oamp.csr` file, which you generated in step 2 on page 196.
   c. Click **OK** to generate the `.pem` file .
6. In the SSH console, run the **`openssl`** command to convert the `.pem` file to a `.pfx/.p12` file.

   The following is an example of the command:

   ```
   sudo openssl pkcs12 -export -out <.p12 file name>-in <.pem file name>.pem -inkey
   oamp.key -passout pass:<password>
   ```

# Importing client certificates into web browsers

## About this task

Use this procedure to import client certificates to the Google Chrome, Internet Explorer, or Mozilla Firefox web browser. This is an optional procedure. After you perform this procedure, you will automatically be logged in to the web administration portal. The system will bypass the Login screen.

## Before you begin

On the HTTP Clients tab, set **OAMP** to one of the following:

- **REQUIRED**: For certificate authentication.
- **OPTIONAL**: For certificate or password authentication.

For information on **OAMP** options, see Available certificate validation options on page 197.

## Procedure

1. Navigate to the appropriate location in your web browser:
   - From Google Chrome, navigate to **Settings** > **Show advanced settings** > **Manage certificates**.
   - From Internet Explorer, navigate to **Tools** > **Internet options** > **Content** > **Certificates**.
   - From Mozzila Firefox, navigate to ≡ > **Options** > **Advanced** > **Certificates** > **View Certificates**.
2. Click **Import** to import the certificate to your browser.

   When prompted for a password, enter the same password that was used in the **openssl** command to convert the `.pem` file to a `.pfx` or `.p12` file.

   **Tip:**

   To override the certificate authentication, in the SSH console, set `com.avaya.cas.common.certificateauth` to `0` as follows:

   ```
   CATALINA_OPTS="$CATALINA_OPTS -Dcom.avaya.cas.common.certificateauth=0"
   ```

# Available certificate validation options

| Name | Description |
|---|---|
| **OPTIONAL** | Enables the Avaya Aura® Web Gateway to validate certificates presented by the clients to establish a secure HTTP connection with the Avaya Aura® Web Gateway. |
| **NONE** | Prevents the Avaya Aura® Web Gateway from performing any validation on certificates presented by the clients. If you select this option, the client cannot perform trusted hosts-based authentication with the Avaya Aura® Web Gateway. |

*Table continues…*

| Name | Description |
|---|---|
| **OPTIONAL_NO_CA** | Enables the Avaya Aura® Web Gateway to validate certificates presented by the clients. However, the Avaya Aura® Web Gateway does not require such certificates to be signed or issued by a trusted Certificate Authority (CA). |
| **REQUIRED** | Ensures that the clients present a valid certificate that is signed or issued by a trusted CA to establish a secure HTTP connection with the Avaya Aura® Web Gateway. |

# Glossary

| | |
|---|---|
| **Busy Hour Call Attempts** | The maximum number of calls supported for one hour in peak traffic conditions. |
| **Cassandra** | Third party NoSQL database, which is used by Avaya Multimedia Messaging to store messaging data and configuration information. For more information, see https://cassandra.apache.org/. |
| **Domain Name System (DNS)** | A system that maps and converts domain and host names to IP addresses. |
| **Fully Qualified Domain Name (FQDN)** | A domain name that specifies the exact location of the domain in the tree hierarchy of the Domain Name System (DNS). |
| **Network Time Protocol (NTP)** | A protocol used to synchronize the real-time clock in a computer. |
| **Secure Shell (SSH)** | Secure Shell (SSH) is a group of standards and an associated network protocol that the system can use to establish a secure channel between a local and a remote computer. SSH uses public-key cryptography to mutually authenticate a user and a remote computer. SSH uses encryption and message authentication codes to protect the confidentiality and integrity of the data that is exchanged between the two computers. |
| **Simple Network Management Protocol (SNMP)** | A protocol for managing devices on IP networks. |
| **SSL (Secure Sockets Layer) Protocol** | The SSL protocol is the leading security protocol on the Internet. It runs above the TCP/IP protocol and below higher-level protocols such as HTTP or IMAP. SSL uses TCP/IP on behalf of the higher-level protocols and, in the process, allows an SSL-enabled server to authenticate itself to an SSL-enabled client. |
| **TCP** | Transmission Control Protocol. |
| **TLS** | Transport Layer Security |
| **UDP** | User Datagram Protocol. This is a communication method, similar to TCP. |

# Index

## A



## C

## D

## E



## F



## G



## H



## I

## K



## L



## M



## N



## O



## P



## R



## S

## T



## U

## V



## W