# Deploying Avaya Aura® Conferencing: Advanced installation and configuration

Release 8.0.6
May 2018

### 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. 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 Designated Processor that hosts 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 on a number of Designated Processors up to the number indicated in the order. 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.

Named User License (NU). You 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. “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.

### 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. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

### Third Party Components

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

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

### Service Provider

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

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

### Compliance with Laws

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

### Preventing Toll Fraud

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

### Avaya Toll Fraud intervention

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

### Security Vulnerabilities

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

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

### Downloading Documentation

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

### Contact Avaya Support

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

### Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from

Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

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

Java is a registered trademark of Oracle and/or its affiliates.

# Contents

# Chapter 1: An Introduction to Avaya Aura® Conferencing

## About this document

This document provides an overview of the components and services that comprise the Avaya Aura® Conferencing solution. This document also contains technical specifications and requirements, and a list of procedures required to install and configure this solution. This document describes the procedures to perform the initial installation and deployment of Avaya Aura® Conferencing Application Server software and Avaya Aura® Media Server software.

## Related resources

### Documentation

The following table lists the related documents for Avaya Aura® Conferencing. Download the documents from the Avaya Support website at http://support.avaya.com.

The Avaya Support website also includes the latest information about product compatibility, ports, and Avaya Aura® Conferencing releases.

**Related links**

Overview on page 21
Implementation on page 21
Administration on page 22
Reference on page 22

## Overview

| Document number | Title | Use this document to: | Audience |
|---|---|---|---|
| 04-604343 | *Avaya Aura® Conferencing Overview and Specification for Avaya Aura®* | Understand the high-level features and functionality of the product. | Customers, business partners, and services and support personnel |
| 04-604344 | *Avaya Aura® Conferencing Overview and Specification for Turnkey* | Understand the high-level features and functionality of the product. | Customers, business partners, and services and support personnel |
| 04-604323 | *Avaya Aura® Conferencing Solution Description for Small and Medium Enterprises* | Understand the high-level features and functionality of the solution. | Customers, business partners, and services and support personnel |
| 04-604328 | *Avaya Aura® Conferencing Solution Description for Medium Enterprises* | Understand the high-level features and functionality of the solution. | Customers, business partners, and services and support personnel |
| 04-604333 | *Avaya Aura® Conferencing Solution Description for Large Enterprises* | Understand the high-level features and functionality of the solution. | Customers, business partners, and services and support personnel |

**Related links**

Documentation on page 20

## Implementation

| Document number | Title | Use this document to: | Audience |
|---|---|---|---|
| 04-604418 | *Deploying Avaya Aura® Conferencing: Basic Installation* | Perform installation and configuration tasks. | Partners, Services, and Support personnel |

*Table continues…*

| Document number | Title | Use this document to: | Audience |
|---|---|---|---|
| 04-604363 | *Deploying Avaya Aura® Conferencing: Advanced Installation and Configuration* | Perform installation and configuration tasks. | Partners, Services, and Support personnel |
| 04-604353 | *Upgrading Avaya Aura® Conferencing* | Perform upgrading and configuration tasks. | Partners, Services, and Support personnel |
| 04-604403 | *Migrating Avaya Aura® Conferencing* | Perform migration and configuration tasks. | Partners, Services, and Support personnel |

**Related links**

Documentation on page 20

## Administration

| Document number | Title | Use this document to: | Audience |
|---|---|---|---|
| 04-604378 | *Administering Avaya Aura® Conferencing* | Perform system-wide administration tasks. | System administrators |
| 04-604403 | *Migrating Avaya Aura® Conferencing* | Perform system-wide security administration and backup/restore tasks. | System administrators |
| 04-604398 | *Maintaining and Troubleshooting Avaya Aura® Conferencing* | Perform maintenance and troubleshooting tasks.<br>Understand logs and fault tracking. | System administrators<br>Partners, Services, and Support personnel |
| — | *Avaya Aura® Conferencing Security* | Perform system-wide security-related administration tasks. | System administrators |

**Related links**

Documentation on page 20

## Reference

| Document number | Title | Use this document to: | Audience |
|---|---|---|---|
| 04–604423 | *Avaya Aura® Conferencing Accounting Records Reference* | Collect information about accounting records | System administrators |

*Table continues…*

| Document number | Title | Use this document to: | Audience |
|---|---|---|---|
| | | | Customers, Partners, Services, and Support personnel |
| 04-604443 | *Avaya Aura® Conferencing Alarms and Logs Reference* | Collect information about alarms and logs, including the alarms and logs families | System administrators<br>Customers, Partners, Services, and Support personnel |
| 04-604444 | *Avaya Aura® Conferencing Operational Measurements Reference* | Collect information about operational measurements | System administrators<br>Customers, Partners, Services, and Support personnel |

**Related links**

Documentation on page 20

## Training

The following courses are available at http://www.avaya-learning.com. In the **Search** field, type the course code, and click **Go** to search for the course.

| Course code | Course title |
|---|---|
| 2U00110O | Selling Avaya Aura® Conferencing Solution Learning Bytes |
| 2U00325O | Avaya Aura® Conferencing 7 L1 Customer Scenario |
| 3U00260W | Designing Avaya Aura® Conferencing |
| 5U00120E | Avaya Aura® Conferencing |
| 3204 | Avaya Aura® Conferencing Implementation and Maintenance Exam |

## 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.

### Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

**Note:**

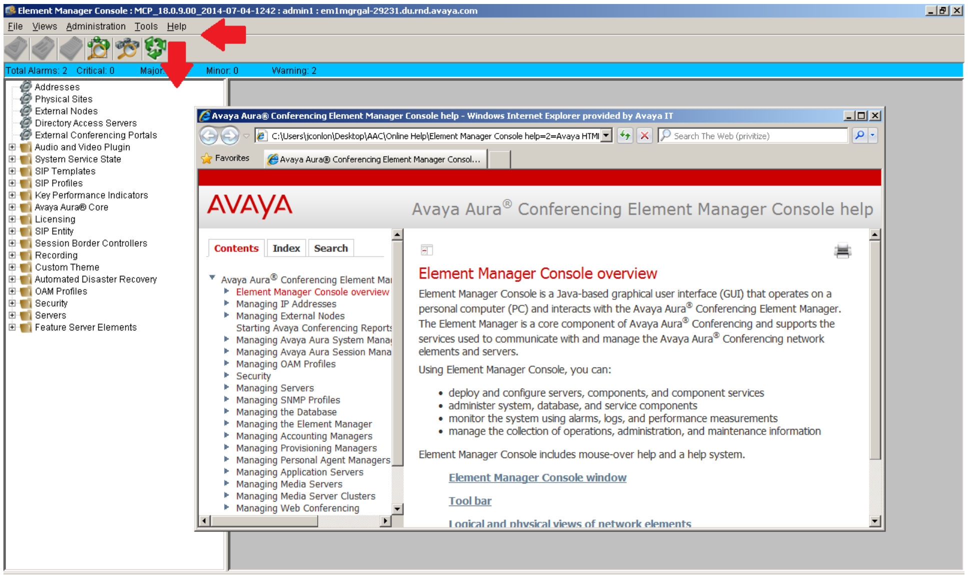
Videos are not available for all products.

## Deploying online help

Avaya Aura® Conferencing contains a number of online help files and online manuals to guide you through the process of installing, configuring, and maintaining your conferencing system. These online help files include:

- Online help for Element Manager
- Online help for the Provisioning Client
- Online help for Reports
- Online help for users of Collaboration Agent

By default, each of these online help packages is fully integrated with the component which it describes. So, for example, if you view help on Element Manager, you can access the Element Manager online help. The Element Manager online help file describes each of the Element Manager fields and describes many of the common procedures that you can perform using the Element Manager interface.


Element Manager Console : MCP_18.0.9.00_2014-07-04-1242 : admin1 : em1mgrgal-29231.du.rnd.avaya.com
File Views Administration Tools Help
Total Alarms: 2 Critical: 0 Major Minor: 0 Warning: 2
Addresses
Physical Sites
External Nodes
Directory Access Servers
External Conferencing Portals
Audio and Video Plugin
System Service State
SIP Templates
SIP Profiles
Key Performance Indicators
Avaya Aura® Core
Licensing
SIP Entity
Session Border Controllers
Recording
Custom Theme
Automated Disaster Recovery
OAM Profiles
Security
Servers
Feature Server Elements
Avaya Aura® Conferencing Element Manager Console help - Windows Internet Explorer provided by Avaya IT
C:\Users\jconlon\Desktop\AAC\Online Help\Element Manager Console help=2=Avaya HTML
Search The Web (privitize)
Favorites
Avaya Aura® Conferencing Element Manager Consol...
AVAYA
Avaya Aura® Conferencing Element Manager Console help
Contents
Index
Search
Avaya Aura® Conferencing Element Ma
Element Manager Console overview
Managing IP Addresses
Managing External Nodes
Starting Avaya Conferencing Reports
Managing Avaya Aura System Mana
Managing Avaya Aura Session Mana
Managing OAM Profiles
Security
Managing Servers
Managing SNMP Profiles
Managing the Database
Managing the Element Manager
Managing Accounting Managers
Managing Provisioning Managers
Managing Personal Agent Managers
Managing Application Servers
Managing Media Servers
Managing Media Server Clusters
Managing Web Conferencing
Element Manager Console window
Tool bar
Logical and physical views of network elements

Element Manager Console overview

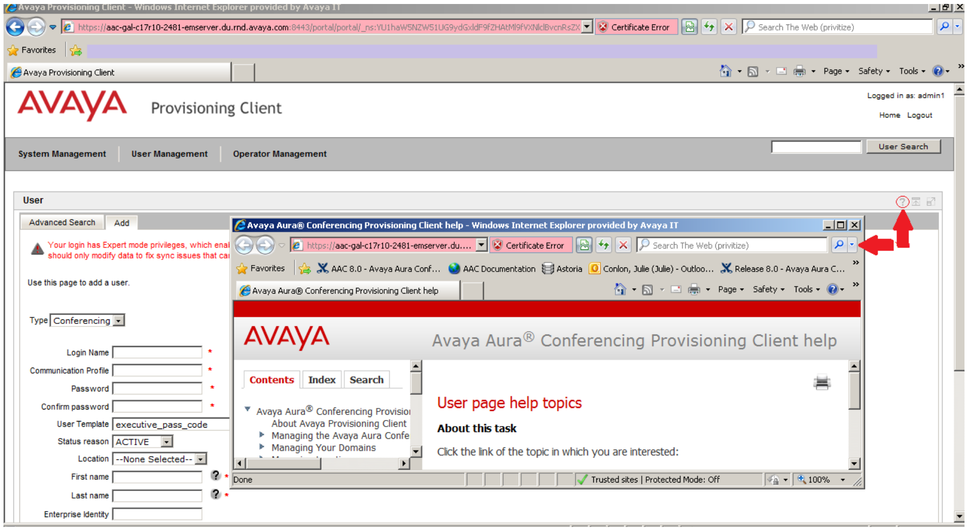
Element Manager Console is a Java-based graphical user interface (GUI) that operates on a personal computer (PC) and interacts with the Avaya Aura® Conferencing Element Manager. The Element Manager is a core component of Avaya Aura® Conferencing and supports the services used to communicate with and manage the Avaya Aura® Conferencing network elements and servers.

Using Element Manager Console, you can:

- deploy and configure servers, components, and component services
- administer system, database, and service components
- monitor the system using alarms, logs, and performance measurements
- manage the collection of operations, administration, and maintenance information

Element Manager Console includes mouse-over help and a help system.

**Figure 1: Online Help for Element Manager**


Avaya Provisioning Client - Windows Internet Explorer provided by Avaya IT
https://aac-gal-c17r10-2481-emserver.du.rnd.avaya.com:8443/portal/portal/_ns:YU1haWSNZWS1UG9ydGxldF9FZHAtMl9fVXNldBvcnRsZX
Certificate Error
Search The Web (privitize)
Favorites
Avaya Provisioning Client
Page Safety Tools
AVAYA
Provisioning Client
Logged in as: admin1
Home Logout
System Management
User Management
Operator Management
User Search
User
Advanced Search
Add
Avaya Aura® Conferencing Provisioning Client help - Windows Internet Explorer provided by Avaya IT
https://aac-gal-c17r10-2481-emserver.du....
Certificate Error
Search The Web (privitize)
Favorites
AAC 8.0 - Avaya Aura Conf...
AAC Documentation
Astoria
Conlon, Julie (Julie) - Outloo...
Release 8.0 - Avaya Aura C...
Avaya Aura® Conferencing Provisioning Client help
Page Safety Tools
AVAYA
Avaya Aura® Conferencing Provisioning Client help
Contents
Index
Search
Avaya Aura® Conferencing Provisio
About Avaya Provisioning Client
Managing the Avaya Aura Confe
Managing Your Domains
Done
Trusted sites | Protected Mode: Off
100%

Your login has Expert mode privileges, which enal should only modify data to fix sync issues that ca

Use this page to add a user.

Type Conferencing

Login Name *
Communication Profile *
Password *
Confirm password *
User Template executive_pass_code
Status reason ACTIVE
Location --None Selected--
First name *
Last name *
Enterprise Identity

User page help topics

**About this task**

Click the link of the topic in which you are interested:

**Figure 2: Online Help for the Provisioning Client**

In the case of the online help for users of Collaboration Agent, Avaya has translated the online help into several languages. The list of available languages conforms with the i18n and L10n (internationalization and localization standards). When users install the Collaboration Agent application, it chooses which language to display based on the computer's locale.

The online help files are packaged within the Avaya Aura® Conferencing software application bundle.

## Support

Go to the Avaya Support website at http://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.

## Audience

The intended audience for this document is:

- Tier 1 Avaya technical support
- Avaya Professional Services
- Authorized Business Partners

You must have the following core competencies:

- The ability to access servers using:
  - a locally attached keyboard and monitor or KVM (Keyboard, Video, Mouse) switch
  - the ssh remote access protocol
- Basic Linux operations:
  - navigating the file system (changing directories)
  - managing the implications of uninformed or careless use of system commands while logged in as the root user
- Basic server tasks:
  - powering servers up
  - powering servers down
  - resetting servers
  - inserting and removing CD-ROM and DVD-ROM disks
- Basic Microsoft knowledge:

  Windows:

  - editing text files
  - creating folders
  - Microsoft Excel:
    - transitioning between worksheets of a workbook
    - entering data into cells

  - copying/pasting between cells and commands, such as Control+c, Control+v, and Edit > Paste Special menu

- The ability to operate a supported Web browser (such as Firefox or Internet Explorer):
  - Interacting with pop-up windows
  - Inspecting and accepting x.509 certificates and installing CA certificates that are presented by the browser
  - Downloading and installing software through the browser
- Basic Public Key Infrastructure (PKI) tasks:
  - Creating Certificate Signing Requests (CSR)
  - Inspecting the details of a certificate
  - Installing Certificate Authority certificates on Windows Certificate Store
  - Installing Personal certificates on Windows Certificate Store
  - Installing Certificate Authority certificates on Firefox Certificate Manager
  - Installing Your Certificates on Firefox Certificate Manager

## Preparing your data using the Avaya Aura® Conferencing Intelligent Workbook

The Avaya Aura® Conferencing Intelligent Workbook is a data collection tool. It is in the Microsoft Excel format. The important tabs are **Checklist**, **Design**, and **Configuration Data** tabs. The other steps and tabs of the workbook are dynamic and depend on the layout selected in the **Design** tab, so they might not be listed as they are listed below. This is an example of typical tabs that might be visible:

- Instructions
- 0-Configuration Data
- 1-OS Linux Install
- 2-OS Patches Install
- 3-ACC Apps Install
- 4-Licensing
- 5-Single sign-on
- 6-Config AAC Services
- 7-Config Avaya Aura
- 8-Provisioning

- 9-Web Conferencing: Enabling Web conferencing
- 10-Video
- A-Flare for Windows and iPad
- B-Update AAC
- C-Apply patches
- FAQ
- Troubleshooting
- Values

# License key

Licensing functionality operates in a different way, depending on your type of Avaya Aura® Conferencing deployment.

You can deploy Avaya Aura® Conferencing with the Avaya Aura® platform. The Avaya Aura® platform consists of Avaya Aura® System Manager, Avaya Aura® Session Manager, and Avaya Aura® System Platform. This type of deployment is called an Avaya Aura® deployment. Alternatively, you can deploy Avaya Aura® Conferencing without the Avaya Aura® platform. This type of deployment is called a Turnkey deployment.

In an Avaya Aura® deployment, licensing is supported on the Application Server and the Media Server. The License key is installed on the Web License Manager (WebLM) server which is co-resident with System Manager. The license key must be obtained prior to starting the deployment.

WebLM is a client/server model where numerous clients can share the same WebLM server and the same license key. For more information, see Installing the license key on on page 171.

In a Turnkey deployment, licensing is also supported by WebLM. However, in a Turnkey deployment, the WebLM server is embedded with Avaya Aura® Conferencing. For more information, see Applying a license key on page 164.

For both solutions, a grace period of 30 days exists for upgrades and new installations. Additionally, new upgrades and installations include a number of default licenses. If the licensing limits are exceeded, Avaya Aura® Conferencing displays full explanatory error messages to users. Licenses must be periodically renewed. If they are not renewed, they expire.

The license monitors:

- Maximum number of provisioned audio, video, and web users
- Maximum number of media servers allowed in the Avaya Aura® Conferencing system
- Maximum number of recording Avaya Aura® Conferencing systems

# Administrative user roles and preconfigured accounts

Roles define operational boundaries (access permissions) for administrators. Administrators can have more than one role, depending on their duties. You assign roles to new administrators when you create their accounts. During server installation, the installation software creates the following user accounts:

| Preconfigured/ Admin accounts | Default password | Preassigned role | Description |
|---|---|---|---|
| ntsysadm | password | System Security Administrator (SSA) role. | The SSA can perform system configuration and specify security attributes such as:<br>• Password configuration<br>• User management<br>• Certificate management<br>• Access control<br>• Antivirus<br>• File System Integrity tools<br>• Network configuration<br>• System backup and restore |
| ntappadm | password | Application Administrator (AA) role | The AA can install the Avaya Aura® Conferencing application software and manage components related to the application. The AA is responsible for installing, maintaining, patching, and upgrading Avaya Aura® Conferencing software only. |
| ntsecadm | password | Security Auditor (SA) role | The SA can collect and view security audit logs and syslogs at the platform level. The SA can also transfer the security logs off the server. |
| ntbackup | password | Backup Administrator (BA) role | The BA can perform only system backups. A BA cannot perform:<br>• any operation on the server except backups.<br>• a system restore—only the SSA or root user can perform a system restore. |
| ntdbadm | password | Database Administrator (DBA) role | The DBA can manage the database schemas and database tools on servers where the database resides. |

*Table continues…*

| Preconfigured/ Admin accounts | Default password | Preassigned role | Description |
|---|---|---|---|
| | | | The server must host the database for this role to be relevant. |
| ntossadm | password | Operational Support System Administrator (OSS) role | Downstream processors can use the ntossadm account with this role to connect to the server and collect OSS logs. |
| admin<br>admin1<br>admin2<br>admin3<br>admin4<br>admin5 | admin<br>admin1<br>admin2<br>admin3<br>admin4<br>admin5 | Unlimited privileges | For expert mode login to Avaya Aura® Conferencing, Element Manager, and Provisioning Manager. |
| init | Not applicable | System Security Administrator (SSA) role and<br>Database Administrator (DBA) role | SSA and DBA account for Avaya Services access. |
| craft | Not applicable | Application Administrator (AA) role | AA account for Avaya Services access |

## Supported Web browsers

Avaya Aura® Conferencing supports the following browsers for Collaboration Agent users and Avaya Aura® Conferencing administrators. Administrators use the following applications to administer and maintain Avaya Aura® Conferencing:

- Element Manager Console
- Provisioning Client
- Avaya Conferencing Reports & Monitors

These administration applications run on the Windows operating system and are not compatible with the Apple OS X operating system.

| Web browser | Operating system |
|---|---|
| Microsoft Internet Explorer 8 and later | Windows 7, 8, 10 |
| Microsoft Edge | Windows 10 |
| Mozilla Firefox version 10 and later | Windows 7, 8, 10 |

*Table continues…*

| Web browser | Operating system |
|---|---|
| | Apple OS X |
| Google Chrome latest version | Windows 7, 8, 10<br>Apple OS X |
| Apple Safari latest version | Apple OS X |

Enable pop-ups in your web browser for Collaboration Agent to function properly.

### Possible limitations in relation to the Audio/Video in Collaboration Agent feature

When running the Audio/Video in Collaboration Agent feature, Google Chrome may demonstrate poor lip synchronization. When Collaboration Agent detects when a user wishes to use the Audio/Video in Collaboration Agent feature in Google Chrome, it displays an information message to inform them of this possible limitation.

In addition, users running Google Chrome for the Mac operating system may experience issues when sharing their desktop. Avaya recommends using Apple Safari or Mozilla Firefox for desktop sharing instead.

**Related links**

Avaya Web Collaboration audio and video plug-in on page 31

## Avaya Web Collaboration audio and video plug-in

In this release of Avaya Aura® Conferencing, there is a new Web-based audio and video client. This client is a browser plug-in which executes within the Web Collaboration Agent client. It enables users to receive their audio and video through the Web. This functionality means that users do not have to dial into the conference using a phone connection. The client is available for all deployment types and can operate seamlessly with other supported clients. Avaya are delivering this feature as a browser plug-in. In previous releases, Avaya delivered a similar but inferior feature using a Flash-based client. The newly enhanced browser plug-in offers an improved audio and video experience and a more intuitive user interface. The older client is still available as part of the software bundle and existing installations can still continue to use the older client. However, Avaya recommends upgrading to the new client for a superior user experience.

For Avaya Aura® Conferencing turnkey deployments, it is likely that most users will receive their audio and video using the new client.

You can control access to the plug-in at a system level. Using this system parameter, you can enable or disable access for all users in your deployment. In addition to this system-wide setting, you can also control access to the Avaya Web Collaboration audio and video plug-in at a user level, by configuring a class of service. For example, you may want to offer the plug-in to some users but not to others. If you enable access to the Avaya Web Collaboration audio and video plug-in, you can choose to inform users of its availability immediately after they join the conference or you can choose not to inform them. If you choose to inform them, Avaya Aura® Conferencing displays a menu and if you choose not inform them, Avaya Aura® Conferencing hides this menu.

If you wish to offer this form of integrated audio and video to external users who reside outside of the enterprise, you must install and configure a Session Border Controller (SBC).

**Related links**

Supported Web browsers on page 30

Web browsers and operating systems that the audio and video conferencing plug-in supports on page 32

## Web browsers and operating systems that the audio and video conferencing plug-in supports

### Web browsers

| Web browsers supported | Web browsers not supported |
|---|---|
| • Mozilla Firefox version 10 and later on Apple OS X and Windows<br>• Microsoft Internet Explorer 8 and later on Windows<br>• Apple Safari latest version for Apple OS X<br>• Google Chrome on Apple OS X and Windows | • Microsoft Internet Explorer for Microsoft Metro<br>• Microsoft Edge<br>• Opera<br>• Any 64–bit version of browsers<br>• All other mobile browsers |

### Operating systems

| Operating systems supported | Operating systems not supported |
|---|---|
| • Windows 7, 32–bit and 64–bit<br>• Windows 8, 32–bit and 64–bit<br>• Windows 10, 32–bit and 64–bit<br>• Apple OS X 10.7 and later | • Older versions of Windows, such as Windows XP<br>• Android<br>• iOS<br>• Linux<br>• Windows Mobile |

### Limitations of the audio and video conferencing plug-in

- The audio and video conferencing plug-in supports only the 32–bit version of web browsers.
- The enterprise network must have a session border controller deployed to support participants who log in to an integrated audio and video conference from outside the network.

**Related links**

Avaya Web Collaboration audio and video plug-in on page 31

# Supported hardware

In this release, Avaya Aura® Conferencing supports the HP ProLiant DL360 G9 for all deployment configurations. Alternatively, if you have an existing HP ProLiant DL360p G8 or HP ProLiant DL360 G7, you can reuse it. If you have existing Dell 610 or IBM S8800 servers, you may be able to reuse them as cascading Avaya Aura® Media Server (MS)'s. However, you cannot reuse the Dell 610 or IBM S8800 servers as Avaya Aura® Conferencing core servers.

The hardware requirements for Avaya Aura® Conferencing are the same whether you are installing the product in an Avaya Aura® deployment or a Turnkey deployment. In both cases, it is the HP ProLiant DL360 G9 server.

| Server type | Supported use |
|---|---|
| HP ProLiant DL360 G9 | Used for new installations of Avaya Aura® Conferencing. |
| HP ProLiant DL360p G8 or HP ProLiant DL360 G7 | Can be reused when upgrading existing Avaya Aura® Conferencing 7.2 deployments to the new release.<br>✱ **Note:**<br>For Large deployments (previously known as Standalone in previous Avaya Aura® Conferencing releases) the server hosting the Element Manager and Database must have more than 12GB of RAM. If your server only has 12GB of RAM, please contact Avaya for a memory expansion kit and apply this kit prior to the upgrade to the new release. For more information on installing and configuring the memory expansion kit, see *Deploying Avaya Aura® Conferencing 7.2.2*, which is available from https://support.avaya.com/. |
| Dell 610 | Can only be used as cascading media servers. |
| IBM S8800 | Can only be used as cascading media servers. |

# Chapter 2: Deployment options

## Deployment layouts

For Avaya Aura® Conferencing, Avaya supports the following deployment layouts:

- SMB simplex
- SMB redundant
- Medium simplex
- Medium redundant
- Large simplex
- Large redundant

**Related links**

Solution specification for small to medium (SMB) enterprises on page 34
Solution specification for medium enterprises on page 37
Solution specification for large enterprises on page 40
Figuring out your ideal deployment configuration on page 48

## Solution specification for small to medium (SMB) enterprises

Avaya has created a customized solution which provides Avaya Aura® Conferencing facilities for small to medium enterprises. This solution:

- Supports up to 1500 users.
- Supports up to 150 concurrent sessions.
- Houses all network elements on a single server.
- Uses lower power CPUs to reduce server cost.
- Includes a recording facility, as an optional feature.
- Supports up to five Avaya Aura® Media Servers in remote sites.
- Supports a deployment that uses a firewall or an Application Delivery Controller (ADC reverse proxy).

**Related links**

Deployment layouts on page 34

Reference configurations for SMB enterprises on page 35
Hardware and software options for SMB enterprises on page 36

## Reference configurations for SMB enterprises

There are two configurations for Avaya Aura® Conferencing:

- SMB simplex
- SMB with redundancy

A redundant configuration incurs additional costs, which the simplex solution does not incur. SMB enterprises require the following to support redundancy:

- A second server
- An ADC, which provides load-balancing

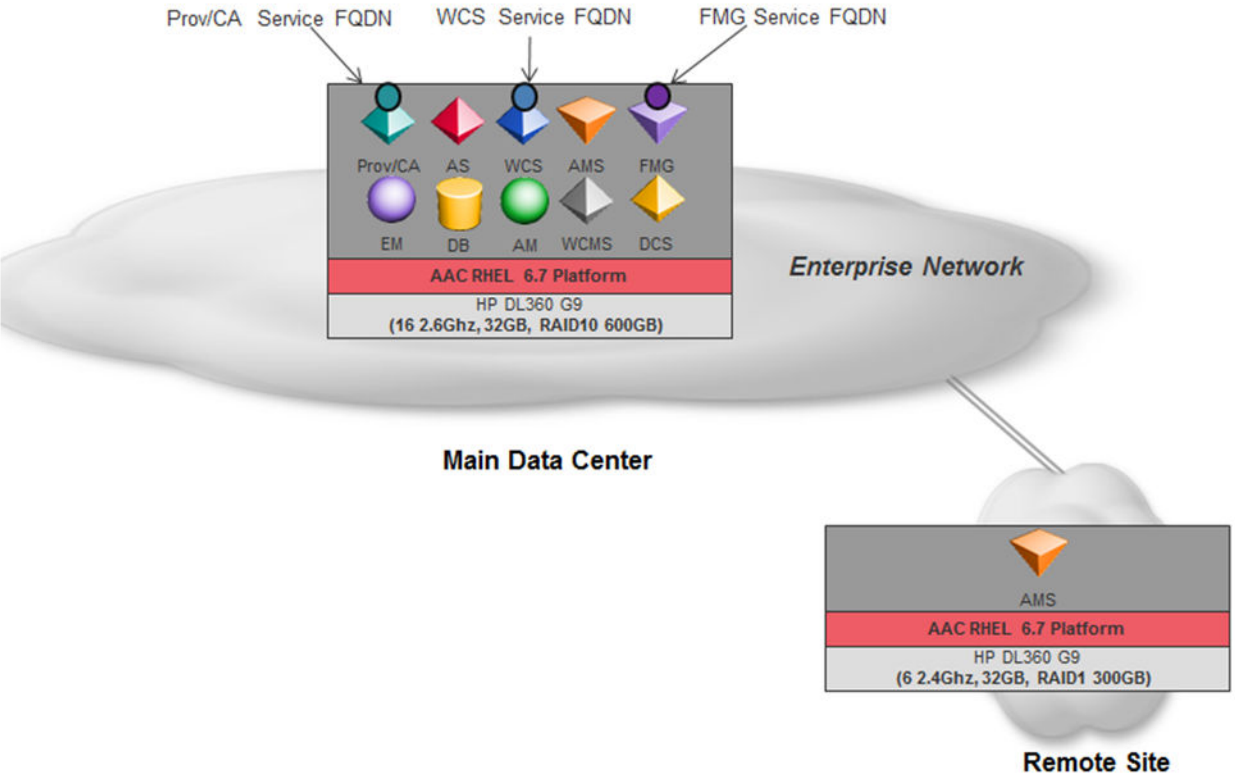


**Figure 3: SMB Simplex Configuration**

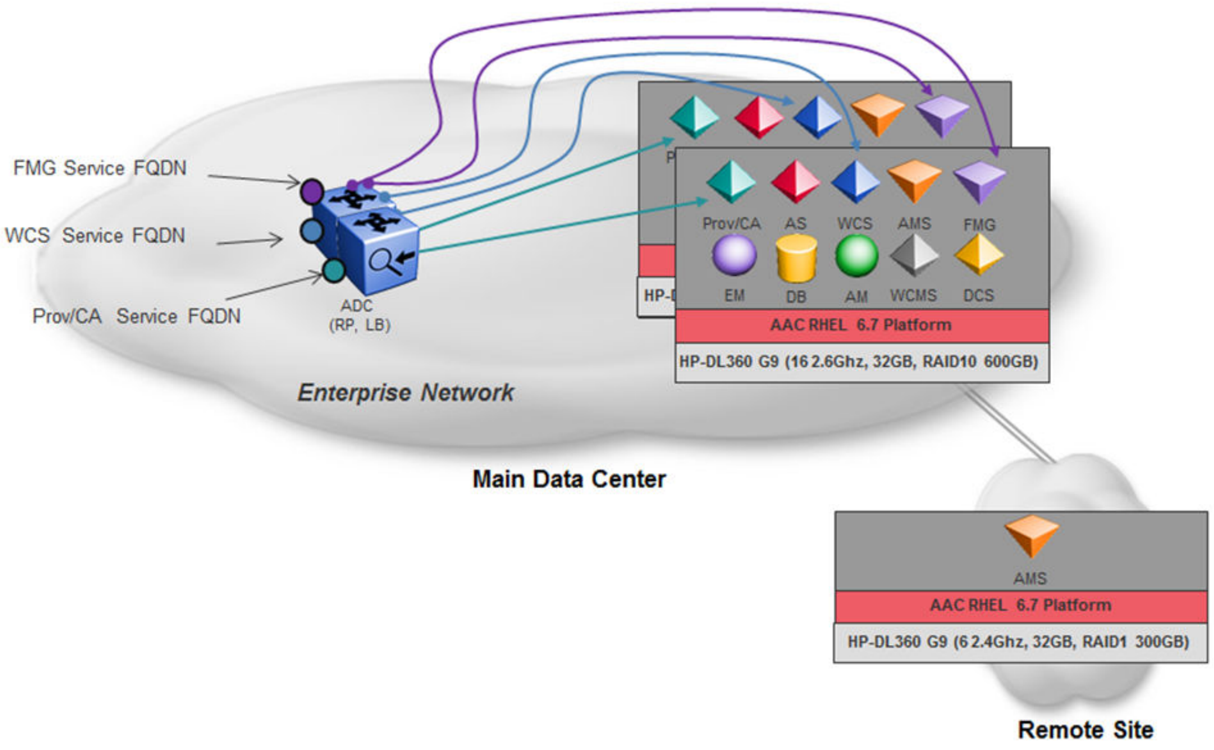


**Figure 4: SMB Redundant Configuration**

### Related links

Solution specification for small to medium (SMB) enterprises on page 34

## Hardware and software options for SMB enterprises

### Hardware

Avaya recommends the following hardware for an Avaya Aura® Conferencing solution in an SMB enterprise.

| Server | Chassis type | CPU | Memory | RAID | NIC | Applications |
|---|---|---|---|---|---|---|
| HP ProLiant DL360 G9 | 1U | • 2xOCT core<br>• 2.6GHz E5-2640v3 | 4x8=32 | 4x300 (RAID10) (600 MB) | • MB<br>• 6 port | Core server |
| HP ProLiant DL360 G9 | 1U | • 1xHEX core<br>• 2.4GHz E5-2620v3 | 4x8=32 | 2x300 (RAID1) (300 MB) | • MB<br>• 6 port | Cascading server<br>Avaya Aura® Media Server |

*Table continues…*

| Server | Chassis type | CPU | Memory | RAID | NIC | Application s |
|---|---|---|---|---|---|---|
| | | | | | | Web Conferencing server |

### Software

The Avaya Aura® Conferencing solution for SMB enterprises is available for deployments that use the Avaya Aura® Private Branch eXchange (PBX). The Avaya Aura® PBX stack includes staging and management software such as System Platform and System Manager.

The Avaya Aura® Conferencing solution for SMB enterprises is also available for deployments that do not use the Avaya Aura® PBX. Deployments that use an alternative PBX are typically called Turnkey deployments. Once installed, the Avaya Aura® Conferencing software behaves in the same way in Avaya Aura® and Turnkey environments.

For more information on Turnkey deployments, see *Overview and Specification for Turnkey*, which is available from https://support.avaya.com/.

The Avaya Aura® Conferencing solution for SMB enterprises is only suitable for bare metal environments. It is not suitable for virtual environments. A 'bare metal' environment refers to the installation of a server directly on to hardware rather than within the host operating system.

**Related links**

Solution specification for small to medium (SMB) enterprises on page 34

## Solution specification for medium enterprises

Avaya has created a customized solution which provides Avaya Aura® Conferencing facilities for medium enterprises. This solution:

- Supports up to 5000 users.
- Supports up to 500 concurrent sessions.
- Houses all network elements on a single server, if required.
- Uses 2.6 GHz CPUs and a RAID 10.
- Includes a recording facility, as an optional feature. The recording feature requires an additional 1.8 TB of storage. As a result of this requirement, Avaya has created a different server order code for a deployment with recording to differentiate it from a deployment without recording.
- Supports up to 10 Avaya Aura® Media Servers in remote sites.
- Supports a deployment that uses a firewall or an Application Delivery Controller (ADC reverse proxy).

**Related links**

Deployment layouts on page 34
Reference configurations for medium enterprises on page 38
Hardware and software options for medium enterprises on page 39

## Reference configurations for medium enterprises

There are two configurations for Avaya Aura® Conferencing:

- Medium simplex
- Medium with redundancy

A redundant configuration incurs additional costs, which the simplex solution does not incur. Medium enterprises require the following to support redundancy:

- A second server
- An ADC, which provides load-balancing

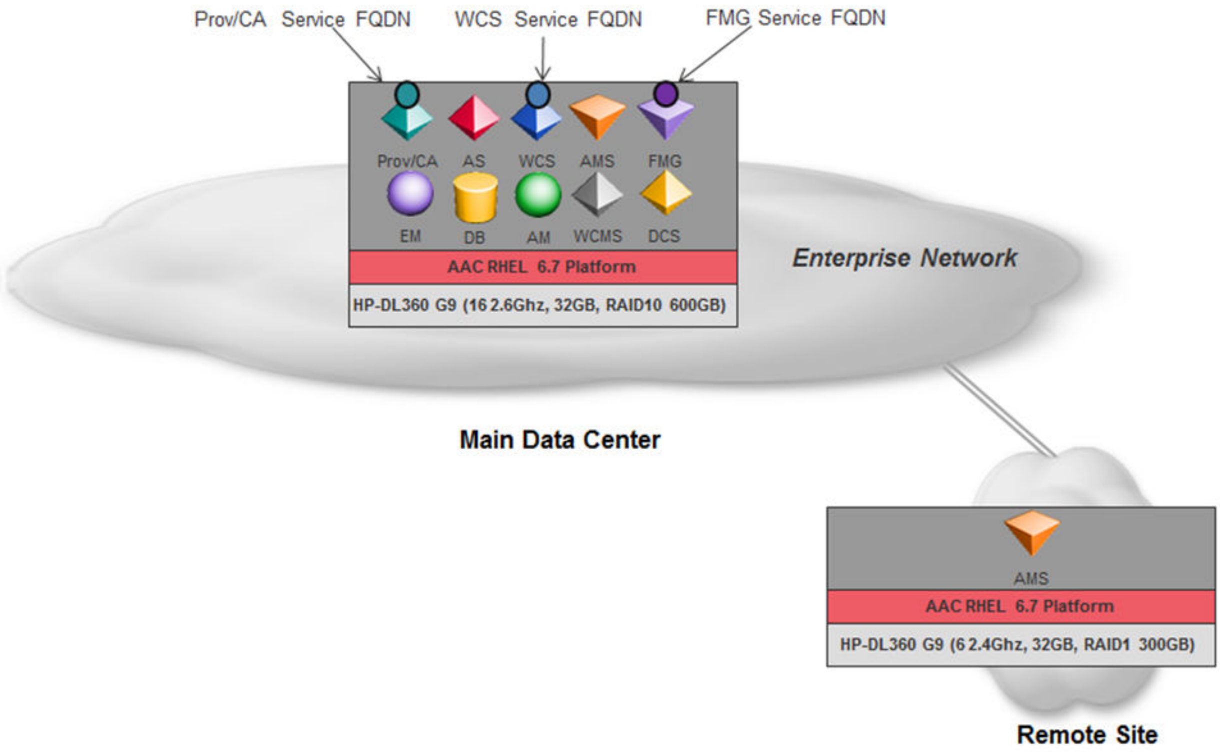


**Figure 5: Medium Simplex Configuration**

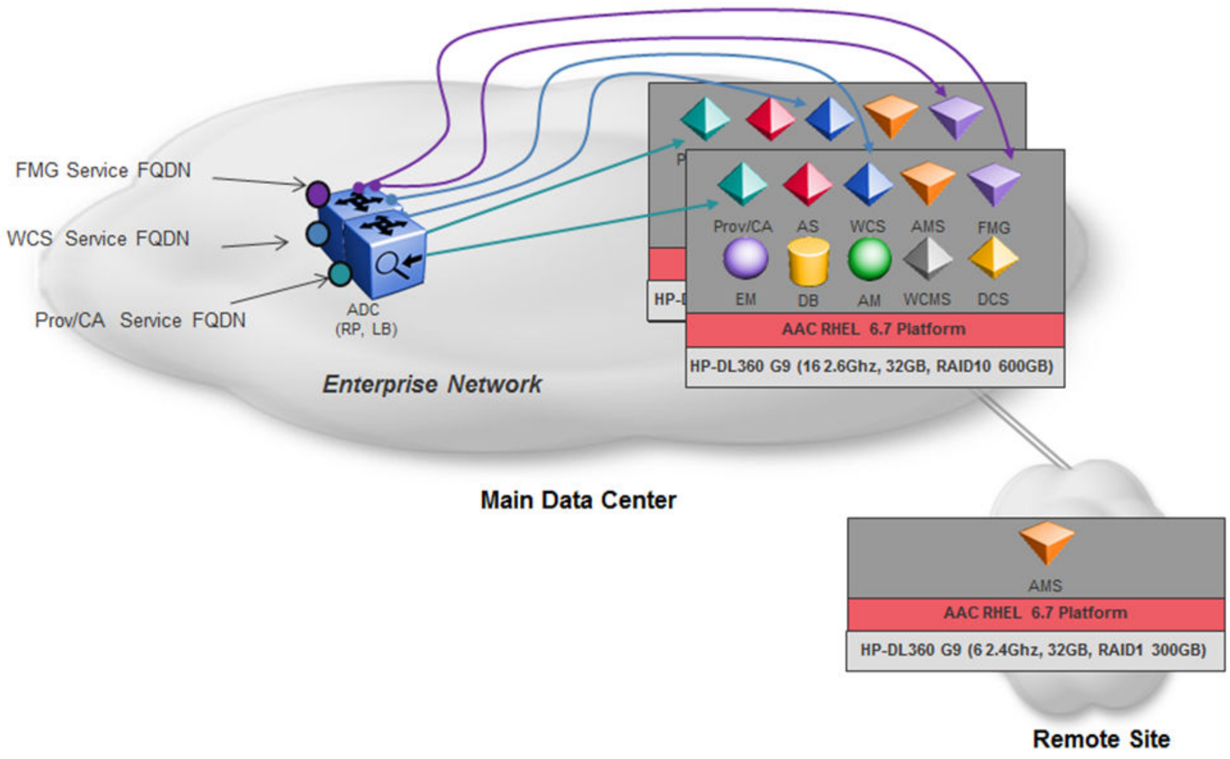


**Figure 6: Medium Redundant Configuration**

### Related links

Solution specification for medium enterprises on page 37

## Hardware and software options for medium enterprises

### Hardware

Avaya recommends the following hardware for an Avaya Aura® Conferencing solution in a medium enterprise.

| Server | Chassis type | CPU | Memory | RAID | NIC | Application s |
|---|---|---|---|---|---|---|
| HP ProLiant DL360 G9 | 1U | • 2xOCT core<br>• 2.6GHz E5-2640v3 | 4x8=32 | 4x300 (RAID10) (600 MB) | • MB<br>• 6 port | Core server when deployed without recording feature[1] |
| HP ProLiant DL360 G9 + Disk Kit | 1U | • 2xOCT core | 4x8=32 | • 4x300<br>• RAID 10 | • MB<br>• 6 port | Core server when deployed |

*Table continues…*

[1] If you want to add the recording feature at a later date, you can buy a disk kit to provide recording functionality. .

| Server | Chassis type | CPU | Memory | RAID | NIC | Applications |
|---|---|---|---|---|---|---|
| | | • 2.6GHz E5-2640v3 | | • (300 MB);<br>• 4x900<br>• RAID 10<br>• (1.8 TB) | | with recording feature |
| HP ProLiant DL360 G9 | 1U | • 1xHEX core<br>• 2.4GHz E5-2620v3 | 4x8=32 | 2x300 (RAID1) (300 MB) | • MB<br>• 6 port | Cascading server<br>Avaya Aura® Media Server<br>Web Conferencing server |

### Software

The Avaya Aura® Conferencing solution for medium enterprises is available for deployments that use the Avaya Aura® Private Branch eXchange (PBX). The Avaya Aura® PBX stack includes staging and management software such as System Platform and System Manager.

The Avaya Aura® Conferencing solution for medium enterprises is also available for deployments that do not use the Avaya Aura® PBX. Deployments that use an alternative PBX are typically called Turnkey deployments. Once installed, the Avaya Aura® Conferencing software behaves in the same way in Avaya Aura® and Turnkey environments.

For more information on Turnkey deployments, see *Overview and Specification for Turnkey*, which is available from https://support.avaya.com/.

The Avaya Aura® Conferencing solution for medium enterprises is suitable for bare metal environments and also for virtual environments. A 'bare metal' environment refers to the installation of a server directly on to hardware rather than within the host operating system. A virtual environment refers to the concealment of the physical characteristics of a computing platform. The virtual environment is enabled by way of VMWare.

**Related links**

Solution specification for medium enterprises on page 37

## Solution specification for large enterprises

Avaya has created a customized solution which provides Avaya Aura® Conferencing facilities for large enterprises. This solution:

- Supports up to 15,000 users.
- Supports up to 1500 concurrent sessions.
- Uses 2.6 GHz CPUs and a RAID 10.
- Includes a recording facility, as an optional feature. The recording feature requires an additional 1.8 TB of storage. As a result of this requirement, Avaya has created a different

server order code for a deployment with recording to differentiate it from a deployment without recording.

- Supports up to 32 Avaya Aura® Media Servers in remote sites. (This total is spread across several server roles.)
- Supports a deployment that uses a firewall or an Application Delivery Controller (ADC reverse proxy).

**Related links**

Deployment layouts on page 34
Reference configurations for large enterprises on page 41
Hardware and software options for large enterprises on page 43

## Reference configurations for large enterprises

There are two large configurations for Avaya Aura® Conferencing: A redundant configuration incurs additional costs, which the simplex solution does not incur. Large enterprises require the following to support redundancy:

- Large simplex
- Large with redundancy
- A second server
- An ADC, which provides load-balancing

Additionally, customers have the option of expanding their system to support up to 30,000 users, running 3000 concurrent sessions, by adding additional servers. This expansion can continue up to a maximum of 150,000 users.

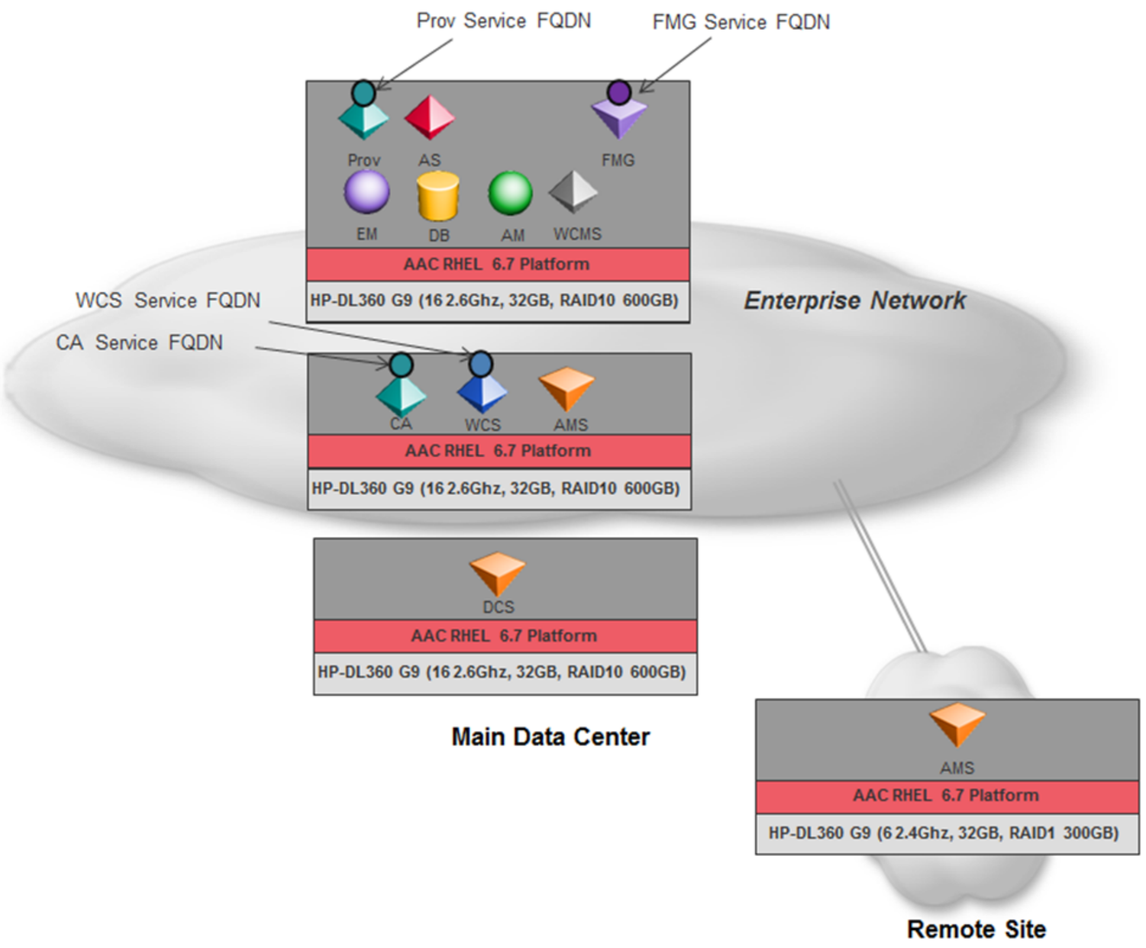


**Figure 7: Large Simplex Configuration**

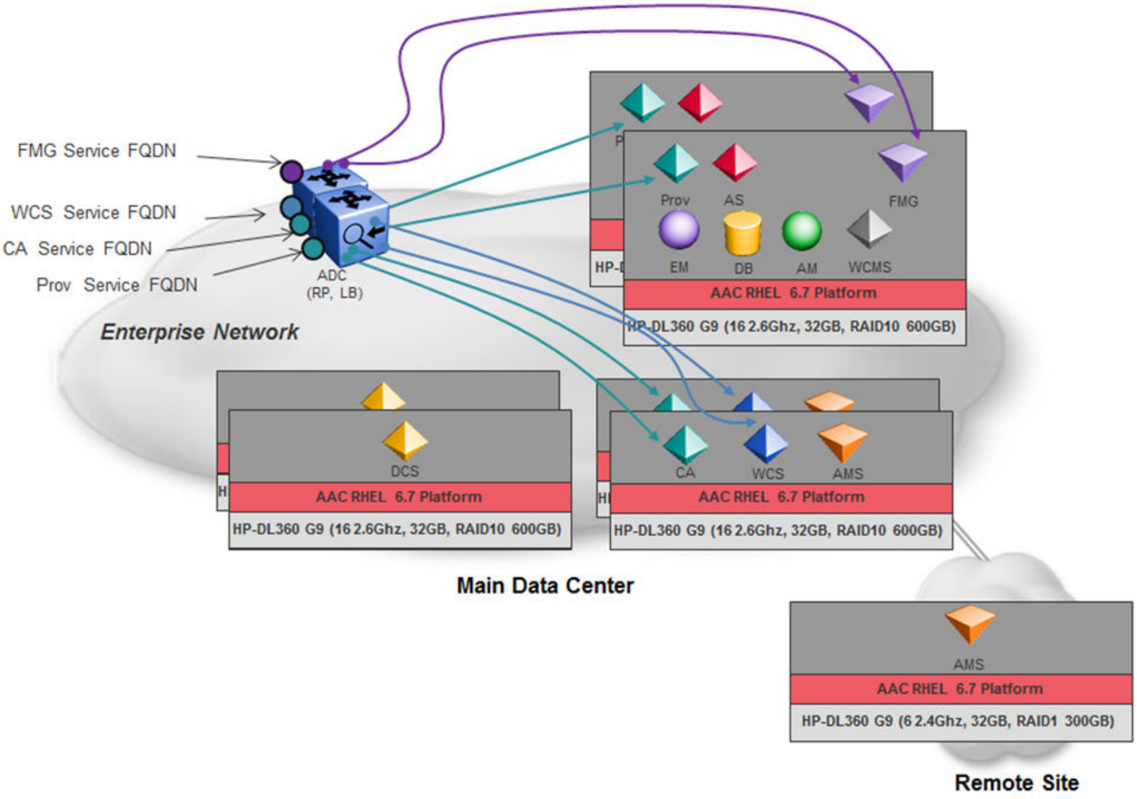


**Figure 8: Large Redundant Configuration**

**Related links**

Solution specification for large enterprises on page 40

## Hardware and software options for large enterprises

### Hardware

Avaya recommends the following hardware for an Avaya Aura® Conferencing solution in a large enterprise.

| Server | Chassis type | CPU | Memory | RAID | NIC | Applications |
|---|---|---|---|---|---|---|
| HP ProLiant DL360 G9 | 1U | • 2xOCT core<br>• 2.6GHz E5-2640 v3 | 4x8=32 | 4x300 (RAID10) (600 MB) | • MB<br>• 6 port | Core Server<br>Avaya Aura® Media Server and Web Conferencing server (WCS) when deployed without recording<br>Hosting Avaya Aura® Media Server when deployed without recording[2] |

*Table continues…*

| Server | Chassis type | CPU | Memory | RAID | NIC | Applications |
|---|---|---|---|---|---|---|
| | | | | | | Hosting WCS<br>Flash Media Gateway for Audio/Video in Collaboration Agent<br>Large Document Conversion Server (DCS)<br>Collaboration Agent (CA) |
| HP ProLiant DL360 G9 + Disk Kit | 1U | • 2xOCT core<br>• 2.6GHz E5-2640 v3 | 4x8=32 | • 4x300<br>• RAID 10<br>• (300 MB);<br>• 4x900<br>• RAID 10<br>• (1.8 TB) | • MB<br>• 6 port | Avaya Aura® Media Server and Web Conferencing server (WCS) when deployed with recording<br>Hosting Avaya Aura® Media Server when deployed with recording |
| HP ProLiant DL360 G9 | 1U | • 1xHEX core<br>• 2.4GHz E5-2620 v3 | 4x8=32 | 2x300 (RAID1) (300 MB) | • MB<br>• 6 port | Cascading server |

### Software

The Avaya Aura® Conferencing solution for large enterprises is available for deployments that use the Avaya Aura® Private Branch eXchange (PBX). The Avaya Aura® PBX stack includes staging and management software such as System Platform and System Manager.

The Avaya Aura® Conferencing solution for large enterprises is also available for deployments that do not use the Avaya Aura® PBX. Deployments that use an alternative PBX are typically called Turnkey deployments. Once installed, the Avaya Aura® Conferencing software behaves in the same way in Avaya Aura® and Turnkey environments.

For more information on Turnkey deployments, see *Overview and Specification for Turnkey*, which is available from https://support.avaya.com/.

The Avaya Aura® Conferencing solution for large enterprises is suitable for bare metal environments and also for virtual environments. A ‘bare metal’ environment refers to the installation of a server directly on to hardware rather than within the host operating system. A virtual environment refers to the concealment of the physical characteristics of a computing platform. The virtual environment is enabled by way of VMWare.

**Related links**

Solution specification for large enterprises on page 40

[2] If you want to add the recording feature at a later date, you can buy a disk kit to provide recording functionality.

# Additional deployment notes

## Enterprise DMZ deployment

For large deployment configurations, you can deploy the Web conferencing server within the Enterprise DMZ of your network firewall. This allows you to connect to an Avaya Aura® Conferencing conference as a member or guest from outside the company firewall while still ensuring a strong and secure network defense. The moderator of a conference can also be located outside of the corporate firewall and still have access to most command functions. You also have the benefit of using Avaya Aura® Conferencing for off-site conferences and events.

**Related links**

Deployment layouts on page 34
Migrating to and from a DMZ on page 260

## Event conferencing and media cascading

Event conferencing requires a dedicated Avaya Aura® Media Server and a dedicated Web Conferencing server. On a bare-metal Avaya Aura® Conferencing system, an event conference can support up to 2,000 active audio sessions per Avaya Aura® Media Server and 1,500 web sessions per Web Conferencing server. For example, you can host a single event conference with a maximum of 2,000 audio sessions and 1,500 web sessions using an Avaya Aura® Media Server and a Web Conferencing server, or you can host multiple event conferences with fewer participants simultaneously using an Avaya Aura® Media Server and a Web Conferencing server as long as the total number of audio sessions does not exceed the maximum of 2,000 and the total number of web sessions does not exceed 1,500.

You can add multiple Avaya Aura® Media Servers and Web Conferencing servers. However, a single event conference will still support a maximum of 2,000 audio sessions and 1,500 media.

You can also have multiple Avaya Aura® Media Servers in one location, enabling you to host multiple event conferences across multiple Avaya Aura® Media Servers in one location. In this scenario, once a conference starts on an Avaya Aura® Media Server, you are limited to the capacity of that Avaya Aura® Media Server. For example, if the first conference has 1,500 audio sessions, then the second conference that starts on that same Avaya Aura® Media Server will be limited to a maximum of 500 audio sessions.

On a VMware Avaya Aura® Conferencing system, the capacity is slightly degraded due to reduced video processing. Instead of 2,000 active audio sessions, a VMWare system has the capacity to support 1,750 concurrent audio sessions. There is no degradation for the Web Conferencing server capacity.

The following table describes the capacities associated with event conferencing.

**Table 1: Target capacities for Event conferencing**

| Servers (dedicated for Event conferencing) | Active audio sessions | Web sessions | Scalable<br>by increasing the number of Event conferences only | Redundancy with an N+m configuration |
|---|---|---|---|---|
| Avaya Aura® Media Server | 2,000 (on a bare-metal system)<br>1,750 (on a VMware system)<br>**Note:**<br>Audio sessions are dedicated to a single server. | — | Yes<br>**Note:**<br>You can increase the number of simultaneous event conferences by adding additional servers. However, each server supports a maximum of 2,000 (bare-metal) or 1,750 (VMware) audio sessions for all event conferences occurring on that server. | Yes |
| Web Conferencing Server (primary and secondary) | — | 1,500<br>**Note:**<br>Web sessions are dedicated to a single server. | Yes<br>**Note:**<br>You can increase the number of simultaneous event conferences by adding additional servers. | Yes |

## Support for cascading

Media cascading reduces the number of media streams travelling across the WAN by consolidating these streams based by location. This technique is applied to both audio and video streams. Media cascading provides bandwidth optimization with no significant reductions in the quality of audio or video. Conferences are scalable with proper configuration and management which is fully transparent to end users. Media cascading is available for event conferences. The combination of these two features — event conferencing and media cascading — provides a very compelling solution for very large global conferences.

If the media cascading location and the location of the hosting media server are different, bandwidth is allocated for the audio media stream to allow for participants joining the conference from other locations without blocking. Network bandwidth is used to transmit/receive audio media streams to/from the Hosting Media Server location, although silence suppression significantly reduces the actual bandwidth received from the hosting location. Video bandwidth for media cascading is only allocated and consumed when it is required in the conference. When all of the participants have joined from a single cascading location, video bandwidth between the Cascading Media Server and the Hosting Media Server is only allocated and consumed if a participant from another location joins the conference.

### Cascading capacity

The following table shows the supported capacity for cascading Avaya Aura® Media Servers for Avaya Aura® Conferencing.

| | Capacity (Audio Sessions) | Capacity (Video Sessions ) | CPUs | Memory (GB) | Storage (GB) | CPU Speed (GHZ) | CPU Reservation (GHZ) |
|---|---|---|---|---|---|---|---|
| VMware system:<br>Cascading Avaya Aura® Media Servers (6 vCPUs) | 540 | 160 | 6 | 16 | 150 | 2.893 | 17.358 |
| Bare-metal system:<br>Cascading Avaya Aura® Media Servers | 600 | 180 | 6 | 16 | 150 | 6 (12 with hyperthreading) | N/A |

In order to successfully support the cascading feature, an event conference requires a dedicated media server for hosting but does not require dedicated media servers at the cascading locations.

For more information on the available hardware options for cascading servers, check the latest list of supported hardware.

**Related links**

Deployment layouts on page 34
Configuring WCS clusters for event conferences on page 256
WCS Clusters for Event Conference tab field descriptions on page 257
Configuring media server clusters for event conferences on page 332

## Integrations with other applications

You can integrate Avaya Aura® Conferencing with a number of applications in the Avaya Aura® product suite. This means that end users can start their own conference or attend other conferences using applications such as Avaya Aura Equinox or Avaya Communicator for Microsoft Lync . These applications are available for Windows, Android, or iOS devices.

For more information on the supported endpoints, see Configuring Audio SRTP on page 586 and for more information on the integration with Microsoft Lync and Avaya Aura Equinox, see Avaya Microsoft Lync Integration overview on page 673 and Overview of Avaya ®Aura Communicator on page 681.

**Related links**

Deployment layouts on page 34

## Disk kit

You can buy a disk kit if you want to add additional storage capacity for your conference recordings. The disk kit is only available for medium or large deployments.

| Server | Chassis type | CPU | Memory | RAID | NIC | Applications |
|---|---|---|---|---|---|---|
| Disk kit | - | - | - | 4x900<br>RAID 10<br>(1.8 TB) | - | Medium and large recording storage |

**Related links**

Deployment layouts on page 34
Recording and memory on page 146

# Figuring out your ideal deployment configuration

To figure out which configuration best suits your requirements for Avaya Aura® Conferencing, it is a good idea to answer four simple questions.

1. Do you need a small, medium, or large-sized solution?

   Within the context of Avaya Aura® Conferencing, a small deployment is defined as a deployment with up to 1500 end users. A medium deployment is defined as a deployment with up to 5000 end users. A large deployment is defined as a deployment with up to 150,000 end users.

2. How are you going to host Avaya Aura® Conferencing?

   Avaya Aura® Conferencing is available to purchase as a software-only solution, deployed using the Open Virtualization Format (OVA) on a VMware platform. Alternatively, Avaya Aura® Conferencing is available to purchase as a hardware (typically, the HP ProLiant DL360 G9) and software solution. Some customers also buy a combination of OVA files and some hardware. So, you can install a virtual solution, using VMware software or you can install Avaya Aura® Conferencing as a “bare metal” solution on the actual physical servers. It is important to note that if you choose a virtualized solution, there are some capacity limitations, independent of the size of solution.

3. How many business site locations do you wish to serve and what is the distance between these locations?

   The global distribution of your end users will drive the number and location of Avaya Aura® Media Server (MS)s.

4. Is your Avaya Aura® Conferencing going to be part of a wider Avaya Aura® solution?

   The Avaya Aura® solution stack consists of Avaya Aura® System Manager and Avaya Aura® System Platform and is often called a Unified Communications (UC) solution. This decision impacts how the system is configured (or data-filled) but should not impact the number of servers required or the applications running on those servers.

It is important to remember that these four questions correspond to four independent factors.

**Related links**

Deployment layouts on page 34

# Chapter 3: Network planning and design considerations

This chapter describes how to plan and design your network for use with Avaya Aura® Conferencing.

**Related links**

## Network considerations

When engineering an Avaya Aura® Conferencing system in an IP network, there are a number of factors that must be taken into consideration. This section provides an overview of the supported Avaya Aura® Conferencing topologies and provides important factors to help create an optimized system design.

**Related links**

Network planning and design considerations on page 50

## Conference usage patterns

Within an organization, conference usage patterns depend on many factors, such as the nature of work, communities of interest, and numerous other variables. Statistics gathered from existing conference solutions can be useful in predicting usage patterns with Avaya Aura® Conferencing.

**Related links**

Network planning and design considerations on page 50

Communities of interest on page 51

Avaya Aura Media Server usage on page 51

### Communities of interest

The communities of interest between different locations are an important factor when designing an optimal conferencing deployment. For example, a location where many participants are joining common conferences will benefit from a locally deployed Avaya Aura® Media Server.

**Related links**

Conference usage patterns on page 51

### Avaya Aura® Media Server usage

Several Avaya Aura® Media Servers can be deployed in a single cluster to support a required number of simultaneous participants. Gathering port usage statistics from an existing conference solution can be beneficial in engineering Avaya Aura® Conferencing. If the enterprise does not have an existing conferencing solution, consider one active user for every ten users to determine the Avaya Aura® Media Server usage.

For more information about the number of Avaya Aura® Media Servers required for a specific number of participants, see *Avaya Aura® Conferencing Overview and Specification*.

**Related links**

Conference usage patterns on page 51

# QoS

QoS provides the ability to configure differentiated services to a user, voice packets, and data packets. QoS guarantees quality to data flow.

To enable QoS, assign a QoS tag when you configure video. If a QoS tag is not assigned , the network uses its best effort for a video transmission.

## Classifying users for QoS

Users can be classified as normal or priority users. To classify priority users, perform the following steps:

1. Set up a priority class of service (CoS) group.
2. Assign priority IP video to the priority CoS group.
3. Assign a user to the priority CoS group.
4. Assign a higher maximum call bit rate for priority IP multimedia.

For users of H.323 endpoints, you can set up separate bandwidth pools within a network region for priority video users.

**Note:**

This document does not include procedures on how to implement QoS.

## DSCP tags

Tagging packets with DSCP tags ensures that, during network congestion, routers drop packets in the following order:

1. Data packets
2. Video packets
3. Audio packets of a video call
4. Audio packets of an audio call

The following table lists the recommended DSCP tags for the different types of packets:

| Packet | DSCP tag |
|---|---|
| Audio | EF – DSCP 46: Expedited Fowarding: RFC-2598 |
| Audio packets in video calls | AF41 – DSCP 34: Assured Forwarding: Class 4, Low Drop Precedence: RFC 2597 |
| Video packets in video calls | AF42 – DSCP 36: Assured Forwarding: Class 4, Medium Drop Precedence: RFC 2597 |
| Data | AF11 – DSCP 10: Assured Forwarding: Class 1, Low Drop Precedence |

**Related links**

Network planning and design considerations on page 50

# Bandwidth capacity

Network wide bandwidth management is performed in the Avaya Aura® architecture by a number of software components that manage bandwidth at various levels of granularity. Session Manager tracks all usage of audio and video bandwidth against the maximum capacity of each location and rejects any requests that exceed the maximum capacity. All bandwidth usage by clients and endpoints involved in multimedia applications that are provided Avaya Aura® Conferencing must first be allocated by the Session Manager so that overall network usage can be properly managed.

To provide a number of advanced capabilities that optimize bandwidth and provide priority-based quality control, Avaya Aura® Conferencing must manage bandwidth usage on an individual location basis and track the characteristics of individual sessions. These sessions are then modified to optimize multimedia sessions from a bandwidth perspective.

To achieve the granularity within Avaya Aura® Conferencing while ensuring overall bandwidth usage is controlled in the network, the Session Manager allows requests for bandwidth allocation updates on an individual location basis. Avaya Aura® Conferencing uses a SIP PUBLISH method to request an update to usage within a minimum/maximum range. Avaya Aura® Conferencing can determine through the Session Manager whether bandwidth can be allocated to allow new sessions or changes in media usage. To maintain an accurate accounting of audio and video bandwidth usage, these updates are requested by Avaya Aura® Conferencing at the start of each new session and then periodically throughout the session, if required.

The Session Manager interface used by Avaya Aura® Conferencing for bandwidth management is also used by other SIP entities that require management of local bandwidth resources and the Avaya Communication Server 1000 when in an integrated site role in the network. This ensures the administrator for Session Manager has a complete view of the bandwidth usage of the network. Detailed scenarios of the Communication Manager and Avaya Communication Server 1000 are not covered in this document.

The following figure shows an architectural overview of the bandwidth management of Avaya Aura® Conferencing with call admission control (CAC).

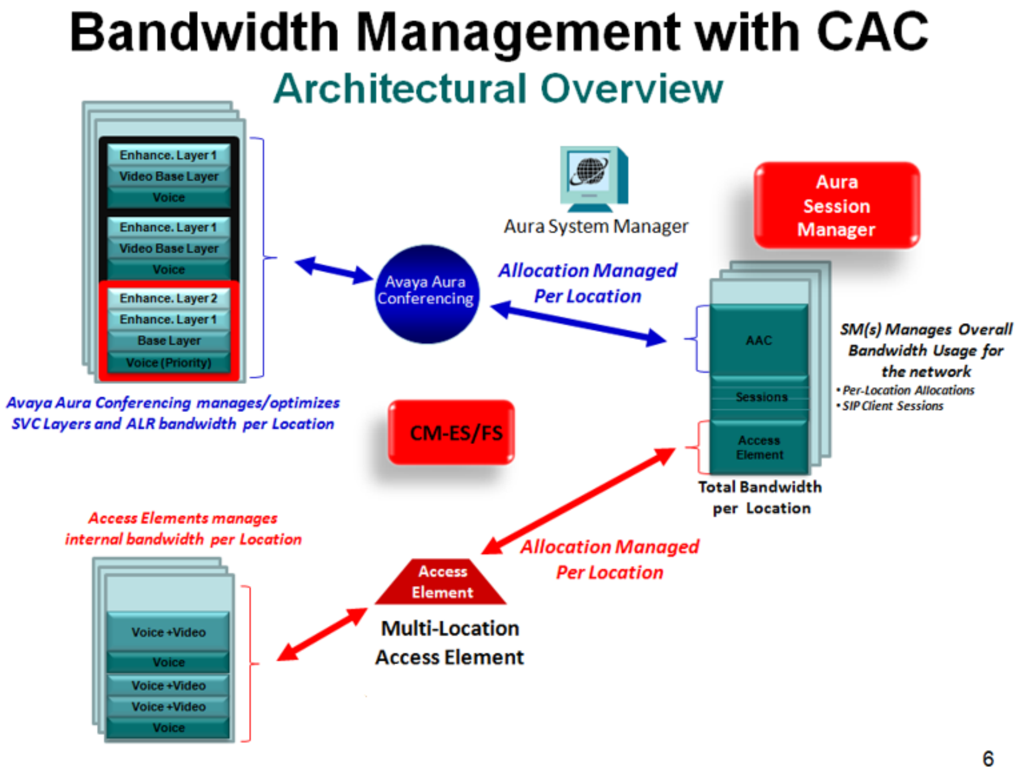

Bandwidth Management with CAC
Architectural Overview
Enhance. Layer 1
Video Base Layer
Voice
Enhance. Layer 1
Video Base Layer
Voice
Enhance. Layer 2
Enhance. Layer 1
Base Layer
Voice (Priority)
Avaya Aura Conferencing manages/optimizes SVC Layers and ALR bandwidth per Location
Avaya Aura Conferencing
Aura System Manager
Aura Session Manager
Allocation Managed Per Location
AAC
Sessions
Access Element
SM(s) Manages Overall Bandwidth Usage for the network
• Per-Location Allocations
• SIP Client Sessions
Total Bandwidth per Location
CM-ES/FS
Access Elements manages internal bandwidth per Location
Voice +Video
Voice
Voice +Video
Voice +Video
Voice
Access Element
Multi-Location Access Element
Allocation Managed Per Location
6

**Figure 9: Bandwidth management with CAC**

### Related links

Network planning and design considerations on page 50

Event conferencing considerations on page 54

## Event conferencing considerations

When considering the network deployment of Event conferencing resources, there are several factors that depend on the nature of the planned scenarios to be supported. These factors are specific to each situation as it occurs. For example, Event conferences that involve a large number of callers from the public require consideration for the point of entry into the network so that the required bandwidth capacities can be accommodated in the network. In this scenario, deployment of an Event conferencing Avaya Aura® Media Server that is collocated with PSTN gateways or session border controls (SBC) would minimize the WAN bandwidth requirements to support the expected calling patterns.

Reliability can also be a key requirement for Event conferences due to the impact of a system failure. Avaya recommends that you place the Event conferencing resources within a highly reliable location.

### Related links

Bandwidth capacity on page 53

# Network impact on audio

As with all real time communications over an IP network, network delays must be managed to avoid user dissatisfaction with the provided audio quality. Generally, end-to-end delay between any two participants in a conference depends on the performance of the network and several other factors. The delays involved when participating in a conference include all network delays between the clients and servers in the media path between any two participants, as well as delays introduced in processing the media.

## Effects of delay on audio quality

The following chart shows the impact of delay on quality as published in the ITU G.114 specification from “Mouth” to “Ear”. For example, all delays including the network, assuming no other impediments, such as packet loss, jitter, compression, and others.

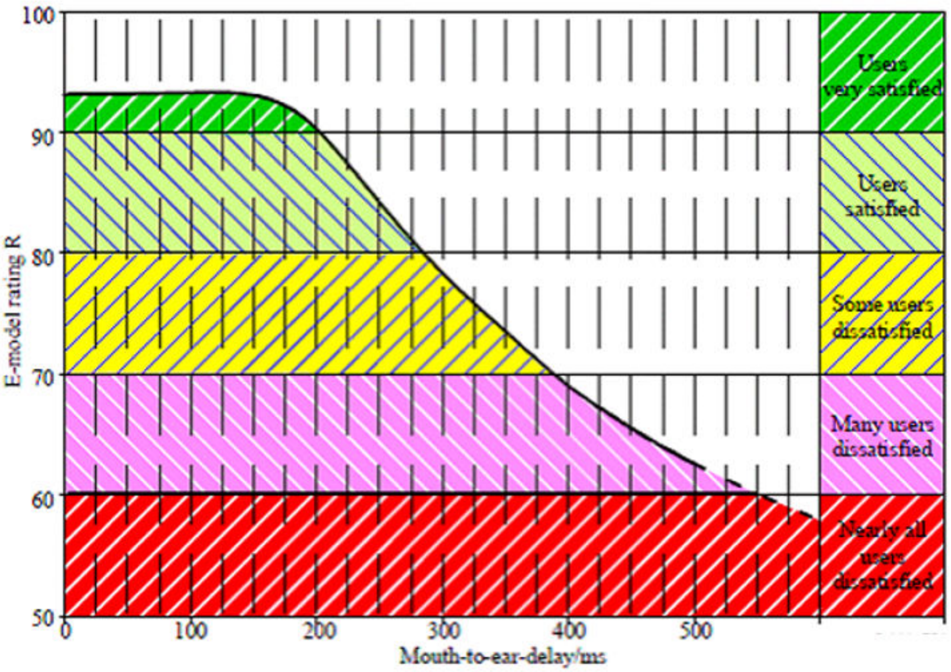


**Figure 10: ITU G.114 Determination of the effects of absolute delay by the E-model**

**Related links**

[Network planning and design considerations](#) on page 50
[Audio delays without media cascading](#) on page 56
[Audio delays with media cascading](#) on page 57

## Audio delays without media cascading

If conferencing using centralized hosting without media cascading, the following figure shows the delays to consider.

Delays to consider:

- d1: Device delay to WAN
- d2: WAN delay to host
- d3: Avaya Aura® Media Server hosting delay
- d4: WAN delay to device
- d5: Device delay to ear

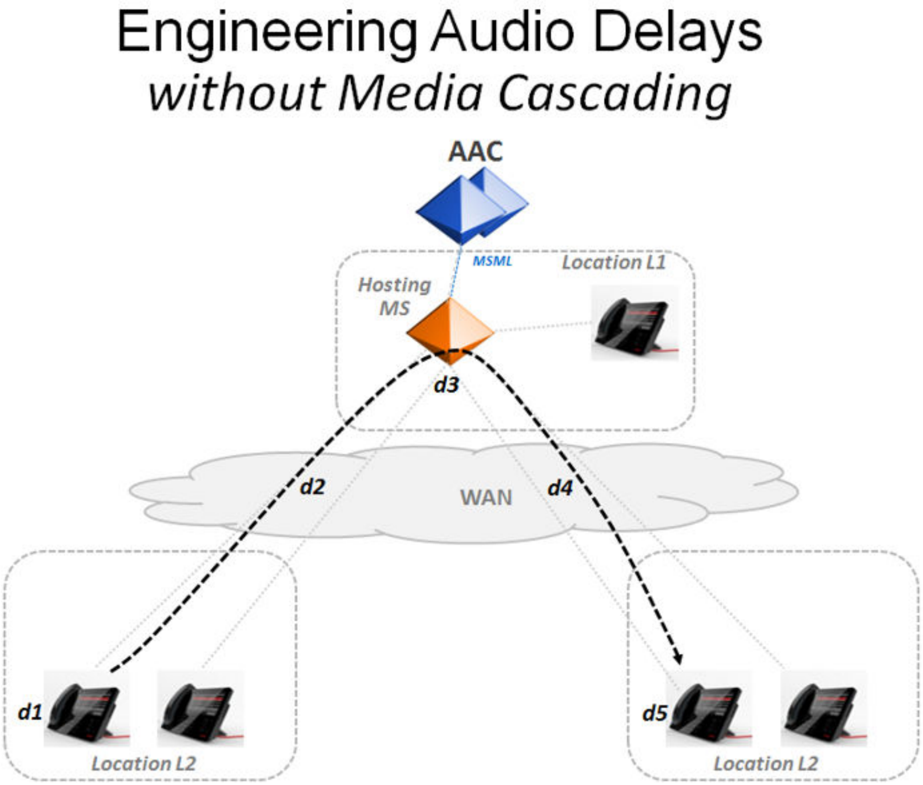


**Figure 11: Engineering audio delays without media cascading**

### Related links

Network impact on audio on page 55

## Audio delays with media cascading

Depending on location, media cascading can contribute to the delays between some participants. The following figure shows the delays to consider when media cascading is enabled.

Delays to consider:

- d1: Device delay to Avaya Aura® Media Server
- d2: Avaya Aura® Media Server delay to WAN
- d3: WAN delay to host
- d4: Avaya Aura® Media Server hosting delays
- d5: WAN delay to cascading location
- d6: Avaya Aura® Media Server delay to device
- d7: Device delay to ear.

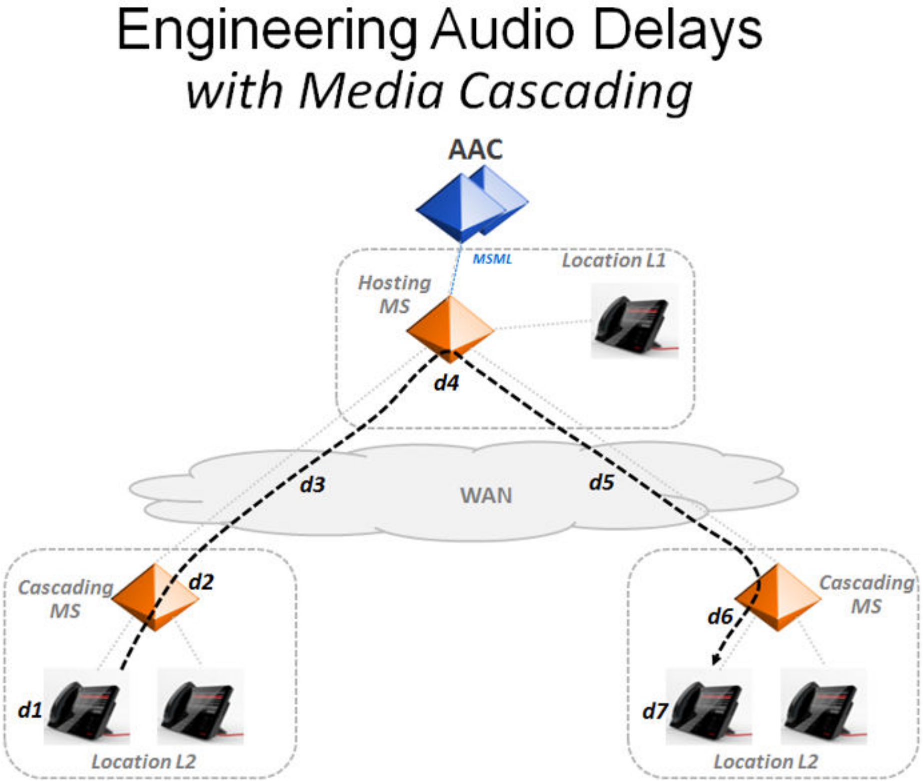


**Figure 12: Engineering audio delays with media cascading**

**Note:**

More complex media flows can involve delays from locations outside of the Enterprise network, such as PSTN gateways, VPN, and Internet. These delays are not shown in the preceding figures but must also be considered where applicable.

**Related links**

Network impact on audio on page 55

## Network impact on video

Multiple network parameters affect the quality of video, such as the bit rate, the frame rate, the packet loss ratio, the content type, the compression method, jitter, and intra-frame coding. Each of these parameters might impact the quality of experience of a user.

### Recommended specifications

The following table lists the recommended values for the network parameters that impact the video quality:

| Network parameter | Recommended value |
|---|---|
| One-way network delay | <= 80 ms to 180 ms |
| Network packet loss for video | <= 0.2 % |
| Latency | < 300 ms |
| Jitter | <= 20 ms |
| Frame rate | >= 26 fps |
| MOS | 4 to 5 |

**Related links**

Network planning and design considerations on page 50

## Service level agreements for audio queues

Avaya recommends that service level agreements be in place to ensure that the delay, jitter, and packet loss characteristics are predictable and managed.

**Related links**

Network planning and design considerations on page 50

# Virtual Private Network location and bandwidth management

The Session Manager typically uses the IP address of a client during registration or the IP address of the media streams described within SIP signaling to determine the current location of a client. If using the Virtual Private Network (VPN) to access to the private network, the address allocated by the VPN infrastructure determines the location to be used for bandwidth management purposes.

The IP mapping to location defined within Session Manager reflects the data path that must be managed from a bandwidth management perspective. This ensures that any limitations in bandwidth at the point of entry to the enterprise network are managed appropriately and provide optimal use of cascading Media Servers within these locations.

**Note:**

The VPN infrastructure adds to the overall delays in media which negatively impacts the overall quality of audio.

**Related links**

Network planning and design considerations on page 50

# Conference dial out

If dial out is enabled for the conference, the moderator can make a dial out call regardless of where the moderator is when joining the conference, for example, at the hosting location or at a cascaded location. The dial out call must be made from the hosting Avaya Aura® Media Server regardless of which Avaya Aura® Media Server the moderator is connected to. The called party joins the conference at that Avaya Aura® Media Server regardless of the called party's location. Therefore, media cascading does not apply to conference dial out calls.

**Related links**

Network planning and design considerations on page 50

# Adhoc conferences

The optimization of media streams by media cascading is applicable only to MeetMe conferences. Adhoc conferences use the hosting Avaya Aura® Media Server without media cascading.

**Related links**

Network planning and design considerations on page 50

# Network location information

Accurate information about the location of a participant is critical to bandwidth management, call admission control, and optimal selection of Avaya Aura® Media Server in a conference. Therefore, all locations within the network must be provisioned within the Session Manager and Avaya Aura® Conferencing. It is also critical that all sessions be associated with one of these locations, either through network address mapping within the Session Manager or by provisioning a SIP Entity Location field within the Session Manager. Sessions that cannot be associated with a location are blocked by Avaya Aura® Conferencing if bandwidth management is enabled because the bandwidth for these sessions cannot be managed within Avaya Aura® Conferencing. An alarm is produced when any blocking of this type occurs. The administrator can then detect, isolate, and repair the configuration of location information.

**Related links**

Network planning and design considerations on page 50

# Voice activity detection and silence suppression

Audio silence detection and suppression (Voice Activity Detection/VAD) can be employed by endpoints that support this capability on audio media streams from client endpoints to the cascading Avaya Aura® Media Server. However, silence suppression cannot be performed by the Avaya Aura® Media Servers on outgoing audio streams to the client endpoints.

**Related links**

Network planning and design considerations on page 50

# Cascading Avaya Aura® Media Server capacity

If a new participant of an existing conference cannot be accommodated by the capacity of an existing Cascading Avaya Aura® Media Server, the new session will block. For audio conferences, each server can support 2,000 or more participants before blocking (using G.729 codec capacity as an example). For video conferences, this limitation depends on the type of video being processed. This limitation is addressed by the scalable conference enhancement by adding another cascading Avaya Aura® Media Server if available, or if another cascading Avaya Aura® Media Server is not available, redirect the new session directly to the hosting Avaya Aura® Media Server.

**Related links**

Network planning and design considerations on page 50

## Blocking due to cascading bandwidth capacity

If Media Cascading is enabled and adequate bandwidth is not available to establish an audio media stream between the cascading Avaya Aura® Media Server and the hosting Avaya Aura® Media Server, participation in the conference is blocked and an announcement provides information about how to join the conference. Users can retry the call if the bandwidth blocking is temporary or dial an alternative number to join the conference (if provided), such as a toll-free number that is always routed through the PSTN.

**Related links**

Network planning and design considerations on page 50

## DTMF signaling by H.323 devices with Communication Manager

Dual tone multifrequency (DTMF) digits are used for conference identification or controls. If sending DTMF digits, the Communication Manager Media Server with indirect media is temporarily placed in the media path so it can provide DTMF signaling within the RTP stream. Bandwidth is temporarily allocated within the location of the Media Server to accommodate DTMF signaling. Avaya recommends that the Communication Manager Media Server, which provides the signaling, to be collocated with the H.323 devices, if possible, to minimize the possibility of blocking the signaling due to bandwidth restrictions.

**Related links**

Network planning and design considerations on page 50

## Direct media with Communication Manager

Use the Direct Media option, if devices that are controlled by an Avaya Aura® Communication Manager participate in Avaya Aura® Conferencing conferences to minimize media path delay and network bandwidth utilization during certain scenarios.

**Related links**

Network planning and design considerations on page 50

## Robustness and reliability

Application Server placement in the network is a critical factor in the overall reliability of the system. This section provides guidelines for server deployment.

**Related links**

[Network planning and design considerations](#) on page 50
[Application server redundancy](#) on page 62
[Avaya Aura Media Server redundancy](#) on page 63
[Web server redundancy](#) on page 64

## Application server redundancy

Avaya Aura® Conferencing supports redundancy. The redundancy option is necessary when reliability of services is critical, especially if a large number of users are dependent on these services. In addition to the redundancy option, application servers must be deployed at network locations with the following attributes:

- highly reliable access to the entire network
- adequate bandwidth capacities for signaling
- highly reliable access to primary and secondary Session Managers that provide session routing and shared bandwidth management interfaces to Avaya Aura® Conferencing

The application servers providing high availability (HA) must be connected within a layer 2 subnet to accommodate sharing of a virtual IP address.

The network design used to deploy application servers must avoid single points of failure in the networking components. For example, LAN switches used to connect redundant servers must also provide network redundancy, including items such as switches and power sources. See the following figure for a redundant network design. Capacity engineering of servers, such as Avaya Aura® Media Server, Web servers must consider the availability of resources in the event of any single networking component failure.

In a redundant deployment, active sessions are retained when a failure occurs on the primary application server. After a five second detection time expires on the primary application server, the secondary application server detects the failure and takes over the active role within about one minute after the initial failure. During this recovery time period, users do not receive any feedback from the application server and any attempts to establish a new session fail.

Avaya Aura® Conferencing maintains interfaces with primary and secondary Session Managers for routing of SIP sessions and managing of network bandwidth. Upon loss of connectivity to the primary Session Manager, current sessions are lost and new sessions are routed to Avaya Aura® Conferencing using the secondary Session Manager. Bandwidth allocations for Avaya Aura® Conferencing are republished to the secondary Session Manager so that network bandwidth management can resume.

**Related links**

[Robustness and reliability](#) on page 61

## Avaya Aura® Media Server redundancy

Avaya Aura® Media Server deployment can provide several forms of redundancy that improve the reliability of services in the network.

**Related links**

Robustness and reliability on page 61
Hosting locations on page 63
Cascading locations on page 63
Locations with Media cascading on page 63

### Hosting locations

Multiple Avaya Aura® Media Servers can be placed in a cluster to provide n+1 load-sharing redundancy of Avaya Aura® Media Servers used for hosting conferences. In the event of a Media Server failure, existing sessions in the conference currently hosted by the server are released and new sessions that arrive are allocated resources from the operational servers.

**Related links**

Avaya Aura Media Server redundancy on page 63

### Cascading locations

Multiple cascading Avaya Aura® Media Servers can be placed in a cluster to provide n+1 load balanced redundancy for Media Servers. In the event of a failure of an Avaya Aura® Media Server, existing sessions using the failing cascading Avaya Aura® Media Server is released and new sessions are allocated resources from the operational servers.

**Related links**

Avaya Aura Media Server redundancy on page 63

### Locations with Media cascading

Multiple Avaya Aura® Media Servers can be placed within a location using media cascading to provide additional capacity and reliability. In the event of a failure of an Avaya Aura® Media Server, the other servers within the cluster are used for the arrival of new sessions. You can use this approach in a location where there are a large number of users or when you need to continue to use media cascading after a server failure.

If a single Avaya Aura® Media Server is deployed at a location using media cascading, failure of the Avaya Aura® Media Server causes new sessions to be redirected to the hosting Avaya Aura® Media Server directly. If bandwidth management call admission control (CAC) is applied, new sessions can overflow to the PSTN when bandwidth is not adequate for the session to proceed over the IP network.

**Note:**

This assumes the Avaya Aura® network is provisioned to provide this behavior.

**Related links**

[Avaya Aura Media Server redundancy](#) on page 63

## Web server redundancy

The Web server supports redundancy options that are used when reliability of n+1 services is critical, especially if a large number of users are dependent on these services. In addition to the using high availability (HA) options, application servers must be deployed at network locations with the following attributes:

- highly reliable access to the entire network
- adequate bandwidth capacities for signaling

The HA options for the Web server are defined based on the network elements running on them. The Web conferencing server on the failed unit are dropped. After the user reconnects, the application server directs them to an active Web conferencing server, assuming there is enough capacity on the remaining active units.

The Web conferencing management server network element supports an active-backup redundancy, and is deployed in a 1+1 configuration. During a failure, all active library sharing sessions stop working; however, you can restart the sharing and the Web conferencing server automatically switches over to the backup Web conferencing management server.

The Collaboration Agent network element supports an active-active redundancy, and is deployed in an n+1 configuration to maintain the desired capacity in the event of a failure. During a failure, any active sessions being hosted on the failed unit are dropped. If the user reconnects, the load balancer directs them to an active Collaboration Agent manager, assuming that there is enough capacity on the remaining active units.

To avoid a single point of failure, deploy the load balancer in a redundant model. Most load balancers support an active-backup redundancy and are deployed in a 1+1 configuration. To review the supported redundancy models, see your respective load balancer documentation. For more information about configuring a load balancer, see the document for *Deploying Avaya Aura® Conferencing*.

**Related links**

[Robustness and reliability](#) on page 61

## Avaya Aura® Media Server deployment for bandwidth optimization

The optimal deployment topology for Avaya Aura® Media Servers in a conference depends upon the factors described in [Network considerations](#) on page 50. In general, Avaya Aura® Conferencing determines the optimal media path for all video and audio streams involved in conferences, if the location of participating endpoints and the location of the Avaya Aura® Media

Servers is known. Avaya Aura® Conferencing sets up the appropriate media streams that flow between clients and the Avaya Aura® Media Servers and between the hosting/cascading Avaya Aura® Media Servers . These media paths require WAN bandwidth to be allocated at all involved locations for each media path involved prior to setting up the media streams.

You can calculate the WAN bandwidth requirements for various deployment models within a network so that the optimal placement of servers and Media Server roles can be identified.

**Related links**

Network planning and design considerations on page 50
Estimating WAN bandwidth usage on page 65
Hosting locations without media cascading on page 68
Locations without Avaya Aura Media Server on page 69
Estimating bandwidth reductions due to media cascading on page 69
Conference size and media stream bandwidth on page 70
Non-hosting locations with media cascading on page 74
Hosting locations with media cascading on page 74
Multiple hosting locations with media cascading on page 75
Delay engineering guidelines on page 75
Minimizing overall delays with packet time selection on page 78

## Estimating WAN bandwidth usage

The amount of bandwidth required to support participants at a location depends on the deployment model used to provide conference services. The bandwidth required to support conferencing cannot be precisely calculated due to variable factors that can change the calling patterns at any time. However, there are some techniques, as described in the following paragraphs to help determine an estimate for bandwidth requirements.

The distributed Avaya Aura® Media Server architecture of Avaya Aura® Conferencing creates a number of location scenarios, depending on where conferences are hosted for the location and whether media cascading is enabled. These location scenarios include:

**Table 2: Location scenarios**

| Location | Scenario |
|---|---|
| L1 | Hosting locations without media cascading |
| L2 | Locations without Avaya Aura® Media Servers |
| L3 | Hosting locations with media cascading |
| L4 | Non-hosting locations with cascading Avaya Aura® Media Servers. |

For the preceding location scenarios, it is necessary to estimate the peak number of users that will be participating in conferences at each location. This information is used in the various location scenarios for Estimating peak participants by location on page 66 and Calculating WAN bandwidth requirements from peak media streams on page 67.

**Related links**

Avaya Aura Media Server deployment for bandwidth optimization on page 64
Estimating peak participants by location on page 66
Estimating WAN bandwidth requirements from audio streams on page 67
Estimating WAN bandwidth requirements from video streams on page 68
Estimating bandwidth requirements from Web conferencing on page 68

## Estimating peak participants by location

The Erlang-B model can be used to estimate the number of media streams required to support the peak participants at each location, assuming an average usage for each provisioned user, for example, 0.1 Erlang and a probability of blocking, for example P=0.001, as shown in the following table. It is assumed that users are participating in audio conferencing at a rate of 0.1 Erlang, which is roughly equivalent to 10% of the time. For conferencing alone, this example assumes a high usage and is for illustration purposes only. The actual average usage will be different than what is used in the example.

**Table 3: Estimating peak participants by location**

| Location | Provisioned users | Erlang (0.1 per user) | Peak participants (P001) | Peak WAN media streams |
|---|---|---|---|---|
| L1 (hosting) | 5,000 | 500 | 555 | 0 |
| L2 (without Media Server) | 3,000 | 300 | 345 | 345 |
| L3 (without Media Server) | 500 | 50 | 64 | 64 |
| L4 (without Media Server) | 200 | 20 | 30 | 30 |
| All locations hosted at L1 | 8,700 | 870 | 994 | 439 |

The following provides a description of the columns in the preceding table:

- Provisioned users. Shows the number of users that use the conferencing system from a location either directly over the network or through gateways deployed within that location.
- Erlang (0.1 per user). Shows the peak number of participants that is expected for a location given the total usage. This peak is determined by referencing a standard Erlang B traffic table assuming a specific probability of blocking (for example, P=0.001), which provides the number of channels required to support this level of usage. For example, at location L1, 555 media streams are required to support 500 Erlang of usage at a probability of P=0.001.
- Peak WAN media streams. Shows the peak number of media streams that travel over the WAN. In the centralized conferencing model, the example shows the media streams within the hosting location (L1) stay within this location and consume no WAN bandwidth. It assumes that any gateways involved in external calls, either by dialing into the conference or

by dialing out from within a conference, are deployed within the hosting location. Because dialed-out participants are established with media streams from the hosting Avaya Aura® Media Server either directly or through locally deployed gateways, dialed-out participants also remain within the location.

**Related links**

Estimating WAN bandwidth usage on page 65

## Estimating WAN bandwidth requirements from audio streams

After estimating the peak WAN media streams, the total audio bandwidth requirement can be calculated for the codecs being used. The bandwidth estimates for supported audio codecs are listed in the following table.

**Table 4: Bandwidth usage (kbps)**

| Codec/Ptime | 10 ms | 20 ms | 30 ms | 60 ms |
|---|---|---|---|---|
| G.711 | 102 | 83 | 77 | 71 |
| G.729 | 46 | 27 | 21 | 15 |
| G.722 | 102 | 83 | 77 | 71 |
| G.726 | 70 | 51 | 45 | 39 |

SIP clients that are capable of receiving Active Speaker notifications for conferences consume additional bandwidth within the audio media streams for this capability. Audio media streams used for media cascading always enable Active Speaker which results in the bandwidth estimates in the following table.

**Table 5: Bandwidth usage (kbps) with active speaker**

| Codec/Ptime | 10 ms | 20 ms | 30 ms | 60 ms |
|---|---|---|---|---|
| G. 711 | 106 | 85 | 78 | 71 |
| G.729 | 50 | 29 | 22 | 15 |
| G.722 | 106 | 85 | 78 | 71 |
| G.726 | 74 | 53 | 46 | 39 |

For example, using the preceding table, client audio streams using a G.722 codec with a 20 ms packet time without Active Speaker enabled consumes about 83 kbps of bandwidth, while audio media streams used for cascading using a G.722 codec with a 10 ms packet time and Active Speaker enabled consumes about 106 kbps of bandwidth.

**Related links**

Estimating WAN bandwidth usage on page 65

## Estimating WAN bandwidth requirements from video streams

The bandwidth usage of video streams varies widely. The bandwidth usage depends on various factors of an enterprise network, which include:

- Video codecs
- Types of video devices
- Video usage pattern of users
- Locations of users

The following table provides estimates of the bandwidth used by different codecs. These estimates will help you estimate the video bandwidth requirements:

**Table 6: WAN bandwidth requirements from video streams**

| H.264 SVC | Profile-Level-ID | Level | Resolution | Cumulative layer Bitrate (kbps) | Independent layer bitrate (kbps) |
|---|---|---|---|---|---|
| Class C | 42400D | 1.3 | 320 x 180 | 128 | 128 |
| | 42401E | 3.0 | 640 x 360 | 512 | 384 |
| | 42401F | 3.1 | 1280 x 720 | 1536 | 1024 |
| Class D[3] | 42401E | 3.0 | 640 x 360 | 512 | 512 |
| | 42401F | 3.1 | 1280 x 720 | 1536 | 1024 |

**Related links**

Estimating WAN bandwidth usage on page 65

## Estimating bandwidth requirements from Web conferencing

Web conferencing uses a reliable transport protocol and does not use the same network traffic class as audio and video. The bandwidth usage of Web conferencing varies widely. This bandwidth usage depends on various factors, which includes:

- Web conferencing usage pattern of users
- The timing rate of page sharing
- Document library or screen sharing usage pattern of users

**Related links**

Estimating WAN bandwidth usage on page 65

# Hosting locations without media cascading

If media cascading is not enabled for a hosting location, the WAN bandwidth usage is directly dependent on the number of users participating in the conference from locations other than the

[3] For the next release of Avaya Aura Conferencing, Avaya will no longer support Class D. Clients that are limited to 180p will not be able to receive or send video to a Class D conference. Avaya recommends using Class C.

hosting location. Bandwidth within the location is assumed to be adequate and is not managed by theAvaya Aura® system.

To estimate the amount of WAN bandwidth required for users participating in conferences from locations other than the hosting location, see Table 3: Estimating peak participants by location on page 66. Using this table, the peak number of participants using WAN bandwidth at the hosting location (L1) is 439 (L2 + L3 + L4). For more information about calculating the WAN bandwidth requirements at the hosting location (L1) in this deployment model and for the particular assumptions about codecs used, see the *Avaya Aura® Conferencing Product Overview and Specification* document.

For example, assuming that the G.722 audio codec uses a 20 ms packet time, the following calculation shows the amount of bandwidth required at hosting location L1:

L1: 439 X 83 kbp = 36,437 kbps WAN bandwidth.

**Related links**

Avaya Aura Media Server deployment for bandwidth optimization on page 64

## Locations without Avaya Aura® Media Server

With a hosting Avaya Aura® Media Server that is centrally deployed, all participants that are not at the conference hosting location use WAN bandwidth for their media streams. The WAN bandwidth required for locations that do not have an Avaya Aura® Media Server locally deployed can be estimated by determining the peak number of conference participants expected at one time. This WAN bandwidth can be estimated by determining the peak number of users and calculate bandwidth requirements based on the codecs that are to be used. In the following example, locations L2, L3 and L4 have an estimated peak number of participants of 345, 64, and 30 respectively.

For example, assuming that the G.722 audio codec with a 20 ms packet time is used, the amount of bandwidth required at hosting location L1 is:

- L2: 345 X 83 kbps = 28,635 kbps WAN bandwidth
- L3: 64 X 83 kbps = 5,312 kbps WAN bandwidth
- L4: 30 X 83 kbps = 2,490 kbps WAN bandwidth

For more information about calculating WAN bandwidth requirements, see the *Avaya Aura® Conferencing Overview and Specification* document for the codecs to be used.

**Related links**

Avaya Aura Media Server deployment for bandwidth optimization on page 64

## Estimating bandwidth reductions due to media cascading

Media cascading starts to provide benefits when two or more users are participating within a conference. The reduction in bandwidth is significantly higher for large conferences that have more participants sharing a common media stream over the WAN. For individual conferences, the reduction in bandwidth provided by media cascading depends on the number of participants in the conference. For example, conferences that have two participants from a location would have a 50% reduction in WAN media streams while conferences with three participants would have a 67% reduction in WAN media streams, and so on. The following table shows the reduction in media streams in a conference for various participant counts from a single location.

| Participants from the same cascading location | Reduction in media streams (percentage) |
|---|---|
| 2 | 50% |
| 3 | 67% |
| 4 | 75% |
| 5 | 80% |
| 6 | 83% |
| ... | ... |
| 50 | 98% |

If estimating the total WAN bandwidth requirements for a cascading location, you need an estimate for the total number of media streams that remain within the location. One method to estimate local traffic is to assume that conferencing has communication patterns that are similar to other call types with respect to communities of interest. For more information about estimating local traffic, see the *Avaya Aura Conferencing Overview and Specification* document. With this assumption, the number of conferences with at least two participants from the same location can be estimated by assuming that they are proportional to general intralocation (Intercom) usage.

**Related links**

Avaya Aura Media Server deployment for bandwidth optimization on page 64

## Conference size and media stream bandwidth

Conferences that have more than two participants from a cascading location provide even more benefit in media cascading. Ideally, the average distribution of conference sizes is known and can be used to provide the most accurate estimate of expected bandwidth savings due to cascading.

The peak bandwidth capacity requirements for a WAN can influence the cost of a network significantly. A strategy that lowers the peak capacity of the network normally results in cost savings. Bandwidth capacity depends on the number of media streams that are in use during this peak period.

If estimating the conferencing peak bandwidth usage, it is helpful to look at the number of conferences by various sizes when performing analysis. The following figure provides an example of conference statistics showing the number of conferences by various conference sizes. In this example, the number of conferences that exceed four participants is 30 percent.

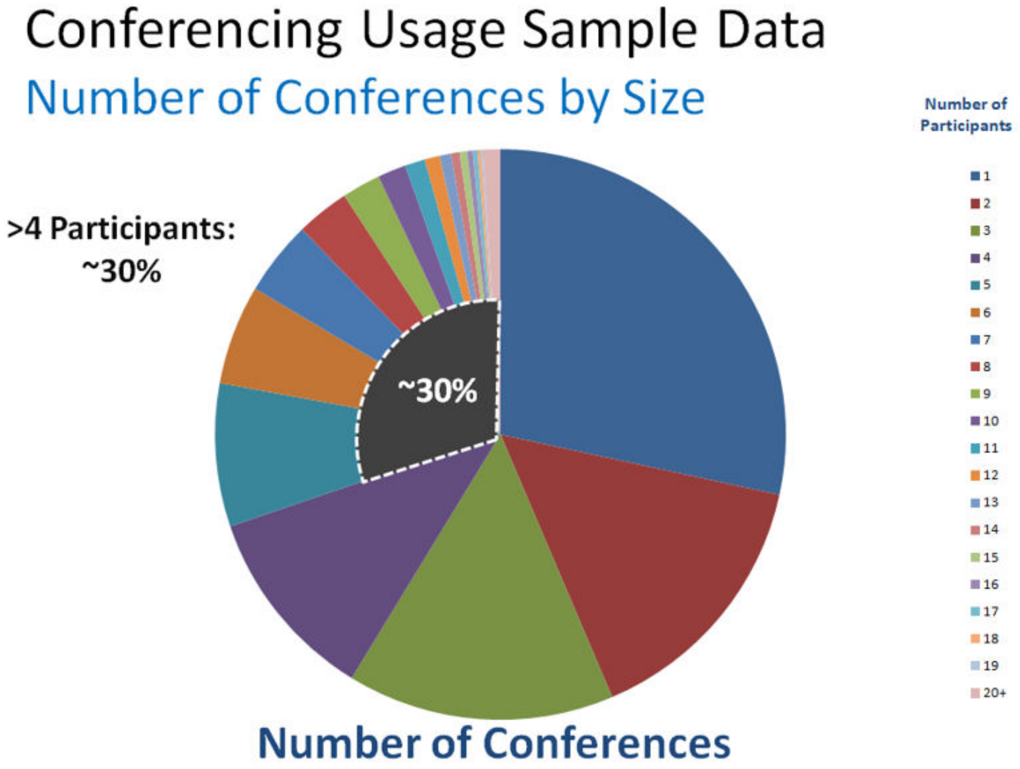


**Figure 13: Conferencing usage sample data by number and size**

In a centrally hosted conferencing topology, the peak bandwidth usage is not only dependent on the number of conferences but also on the total time spent by participants sending or receiving media streams in a conference. Using the same conferencing statistics when taking the total time of participation into consideration, the following figure shows the total participant time spent using bandwidth for media streams. Although there are many smaller conferences, the conferences that are larger than four participants consume about 78 percent of the bandwidth usage.

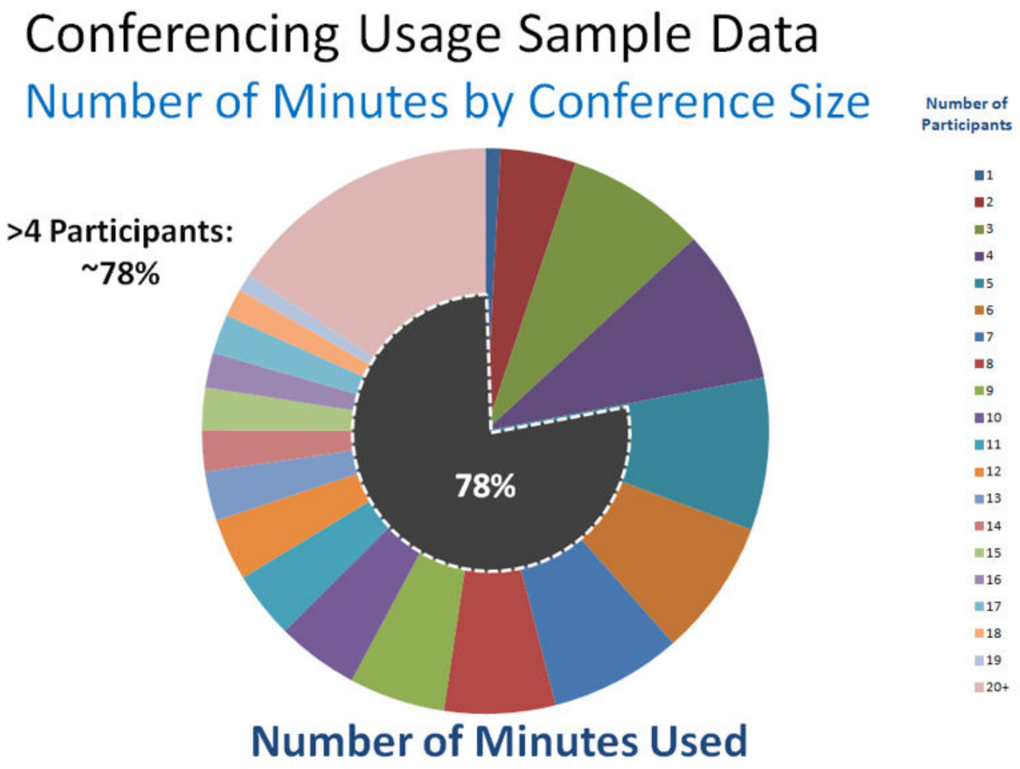


**Figure 14: Conferencing usage sample data by size and number of minutes**

An intralocation factor can be calculated based on the portion of communications that stays within a location. For example, assuming that intralocation (intercom) usage, inbound and outbound traffic for a site are estimated at 40, 30, and 30 Erlangs, respectively, the intralocation factor would be 40 percent. That is, 40 percent of the media streams would have at least two participants within a location.

**Table 7: Reduction in client media streams due to media cascading**

| | Provisioned users | Erlang 0.1 per user | Peak Participants (P001) | Peak WAN Media streams without cascading | Intralocation factor | Intralocation media streams | Media streams used for Intralocation cascading | Total peak WAN media streams |
|---|---|---|---|---|---|---|---|---|
| Location L1<br>(hosting) | 5,000 | 500 | 555 | 0 | — | — | — | — |

*Table continues…*

| | Provisioned users | Erlang 0.1 per user | Peak Participants (P001) | Peak WAN Media streams without cascading | Intralocation factor | Intralocation media streams | Media streams used for Intralocation cascading | Total peak WAN media streams |
|---|---|---|---|---|---|---|---|---|
| Location L2 (cascading) | 3,000 | 300 | 345 | 345 | 40% | (138) | 35 | 242 |
| Location L3 (cascading) | 500 | 50 | 64 | 64 | 40% | (26) | 7 | 45 |
| Location L4 (no Media Server) | 200 | 20 | 30 | 30 | — | — | — | 30 |
| All locations hosted at L1 | 8,700 | 870 | 994 | 439 | — | (164) | 42 | 317 |

In the preceding table, the reduction in client media streams due to media cascading is based on an average of four parties who are participating in each conference, providing an average of 75 percent reduction for intralocation media streams. The reduction can be significantly greater if larger conference sizes are expected during peak traffic periods.

The following provides a description of the columns in the preceding table (See Table 3: Estimating peak participants by location on page 66 for more column descriptions):

- Intralocation factor. Shows the portion of media flows that are expected to remain within a location. This is based on the communities of interest and calling patterns. This factor is used to estimate the number of media streams that benefit from media cascading within conferences. In this example, a factor of 40 percent is assumed.
- Intralocation media streams. Shows the number of media streams between participants within the same location. Calculate by multiplying the intralocation factor by the peak WAN media streams without cascading. For example, in location L2, the intralocation media streams is 40% X 345 = 138.
- Media streams used for intralocation cascading. Shows the number of media streams that are required to carry the intralocation media streams to the hosting Avaya Aura® Media Server over the WAN. It is calculated by applying an average media cascading savings for conferences, such as 75 percent, to the intralocation media streams. For example, in location

L2, 138 media streams can be carried in 138 X 25% = 35 cascading media streams. This is a savings of 103 media streams due to media cascading, that is 138 – 35 = 103.

- Total peak WAN media streams. Shows the total number of media streams that are required to carry all conference media over the WAN. This is calculated by adjusting the total number of media streams without cascading by the savings due to media cascading. For example, in location L2, the savings of 103 media streams reduces the total media streams over the WAN from 345 to 242, that is 345 – 103 = 242.

Assuming the audio codecs in the preceding table, the following calculations show the total bandwidth estimated for locations L1, L2, and L3:

- L1: 317 X 106 kbps = 33,602 kbps (hosting of L1, L3, and L4)
- L2: 242 X 106 kbps = 25,652 kbps
- L3: 45 X 106 kbps = 4,770 kbps

If the network delays are such that cascading media streams with 20 ms packet times can be used, for example, 85 kbps, the bandwidth is reduced further, as shown in the following calculations:

- L1: 317 X 85 kbps = 26,945 kbps
- L2: 242 X 85 kbps = 20,570 kbps
- L3: 45 X 85 kbps = 3,825 kbps

**Related links**

Avaya Aura Media Server deployment for bandwidth optimization on page 64

## Non-hosting locations with media cascading

Locations with media cascading enabled that are not hosting conferences locally, benefit from the shared streams in situations where two or more participants are in the same conference. As shown in Table 7: Reduction in client media streams due to media cascading on page 72, the WAN bandwidth at the cascading location can be estimated by first determining the peak number of media streams expected and adjusting this estimate by the reduction of streams expected due to cascading at the cascading locations. Also, the peak WAN media streams for locations L2 and L3, after adjusting for media cascading, is estimated at 242 and 45, respectively.

**Related links**

Avaya Aura Media Server deployment for bandwidth optimization on page 64

## Hosting locations with media cascading

If media cascading is enabled for locations that are hosted by a central location, WAN bandwidth is reduced at both the hosting location and the cascading location. As shown in Table 7: Reduction in client media streams due to media cascading on page 72, the WAN bandwidth at the hosting location can be estimated by first determining the peak number of media streams expected and adjusting this estimate by the reduction of streams expected due to cascading at all locations using that hosting location.

The hosting location L1 has a reduction in peak media streams of 122, which reflects the total reduction in peak media streams of cascading locations L2 and L3 from 439 to 317.

**Related links**

Avaya Aura Media Server deployment for bandwidth optimization on page 64

## Multiple hosting locations with media cascading

An additional benefit of an Avaya Aura® Conferencing distributed Media Server architecture is the flexibility to select a hosting Avaya Aura® Media Server that is optimal for users within a location. You can then define multiple hosting locations to further optimize network resources. With this deployment model, conferences that include only participants from within the hosting location do not consume any WAN bandwidth.

For example, a conference call with three participants, including one caller using a PSTN gateway and two participants within the same location, does not require WAN bandwidth if the location is hosting the conference. There are many factors that influence the probability of local-only conferencing, including calling patterns and communities of interest, that prevents a general rule that covers engineering of all scenarios. However, if local conferencing can be estimated, the number of media streams used for cascading can be reduced by the number of local conferences for each hosting location.

**Related links**

Avaya Aura Media Server deployment for bandwidth optimization on page 64

## Delay engineering guidelines

The end-to-end delay for media paths can have an effect on the audio quality of conference sessions. For more information, see Network considerations on page 50. Depending on the number of servers in the path, the Media Servers that handle the audio add to the overall delay in the media path. The following table provides a summary of the approximate delays introduced by Avaya Aura® Media Servers for direct and cascaded scenarios, assuming the use of a G.722 codec with 20 ms packet times by the participating clients:

**Table 8: Direct or cascaded hosting delays**

| Direct or cascaded | Avaya Aura® Media Server (MS) packet times |
|---|---|
| Direct hosting: single Media Server | MS1: ~60 ms |
| One cascaded site (two Media Servers) | MS1: ~55 ms<br>MS2: ~50 ms |
| Two cascading sites (three Media Servers) | MS1: ~55 ms |

*Table continues…*

| Direct or cascaded | Avaya Aura® Media Server (MS) packet times |
|---|---|
| | MS2: ~45 ms<br>MS3: ~50 ms |

With a delay introduced within the communications devices, there are also delays caused by the network or Avaya Aura® Media Servers. In the following examples, the device delays are assumed to be approximately 70 ms including both clients involved in the media flow, which is characteristic of the Avaya 9600 series IP Deskphones using a G.722 codec with 20 msec packet times. The delay introduced by other devices is dependent on the client implementation of a number of features, such as jitter buffer management, media handling algorithms, codec in use and packet times.In both figures, the 70 ms delay is shown as 30 ms at the transmitting client and 40 ms at the receiving device.

The following figure shows delay calculations for a media path without media cascading. The following calculation shows the overall delay after determining the values for each type of delay to be considered. A client codec G.722/G.711 is assumed with a packet time of 20 ms.

Delays to consider:

- d1: 30 ms
- d2: 30 ms (60 ms RTD)
- d3: 60 ms
- d4: 30 ms (60 ms RTD)
- d5: 40 ms
- Total 190 ms

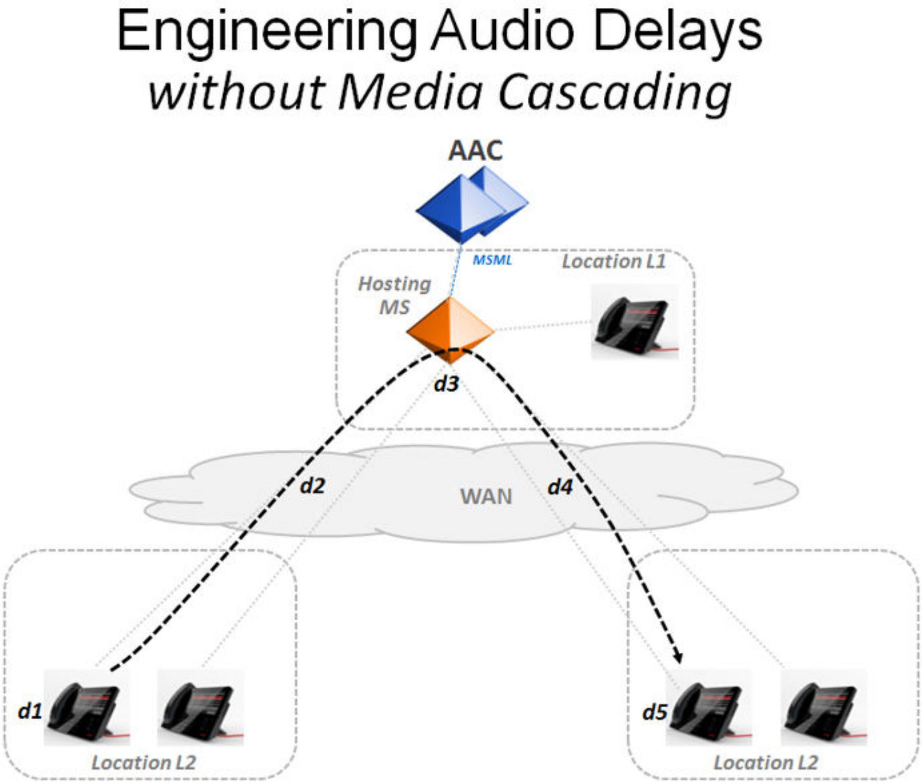
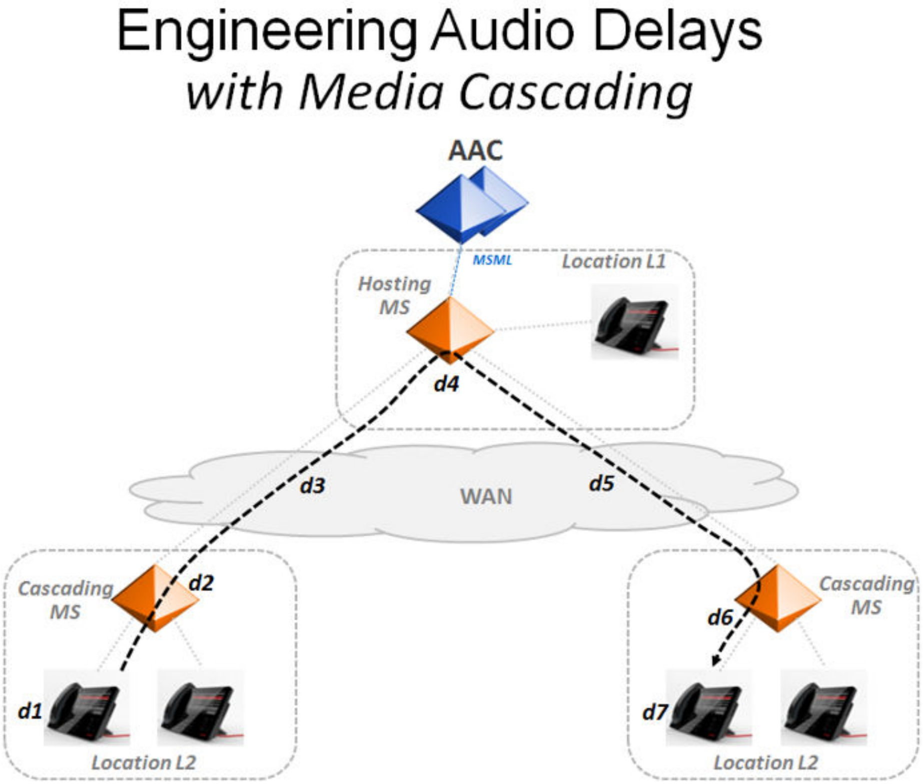


**Figure 15: Engineering audio delays without media cascading**

The following figures shows delay calculations for a media path that includes media cascading. A client codec G.722/G.711 is assumed with a packet time of 20 ms.

Delays to consider:

- d1: 30 ms
- d2: 55 ms
- d3: 30 ms (60 ms RTD)
- d4: 45 ms
- d5: 30 ms (60 ms RTD)
- d6: 50 ms
- d7: 40 ms
- Total 280 ms



For more information about the effect these delays have on the overall audio quality of the conference, see Effects of delay on audio quality on page 55. The additional delay introduced by media cascading is approximately 90 ms, due to the additional buffering and processing required (approximately 150 ms for media processing with cascading compared to 60 ms without cascading). In the preceding figures, the packet time used for the media streams between the cascading Avaya Aura® Media Server and the hosting Avaya Aura® Media Server is assumed to be 10 ms, which reduced the delays in media path when compared to 20 ms packet times.

**Related links**

Avaya Aura Media Server deployment for bandwidth optimization on page 64

## Minimizing overall delays with packet time selection

An approach to consider that further minimizes the delay that is introduced by media cascading is to use a 10 ms codec between the clients and the cascading Avaya Aura® Media Servers

**Note:**

This feature will be available in a future client release.

This approach lowers the delays introduced by all Avaya Aura® Media Servers involved from 150 ms to about 130 ms when compared to a 20 ms packet time.

**Related links**

Avaya Aura Media Server deployment for bandwidth optimization on page 64

## Shared bandwidth management

As described in the Network considerations on page 50, bandwidth management in an Avaya Aura® network is performed by the Avaya Aura® Session Manager with the cooperation of Avaya Aura® Conferencing using a SIP-based shared bandwidth management interface. Bandwidth that is required for an Avaya Aura® Conferencing session must first be allocated through this interface before the session can proceed. Other SIP sessions that are routed through the Avaya Aura® Session Manager can also consume bandwidth from this shared resource pool. This allows network bandwidth to be shared among applications under the control of the Avaya Aura® Session Managers.

Bandwidth that is required for sessions that are controlled within the Communication Manager or the Avaya Communication Server 1000 that are not routed through the Avaya Aura® Session Manager must be managed within the bandwidth management services of these elements until the shared bandwidth management interface is supported by these elements. This requires a portion of the available bandwidth for each network location to be dedicated to the Avaya Aura® Session Manager and a separate portion to be dedicated to the Communication Manager or the Avaya Communication Server 1000 systems.

**Related links**

Network planning and design considerations on page 50

Monitoring bandwidth usage on page 79

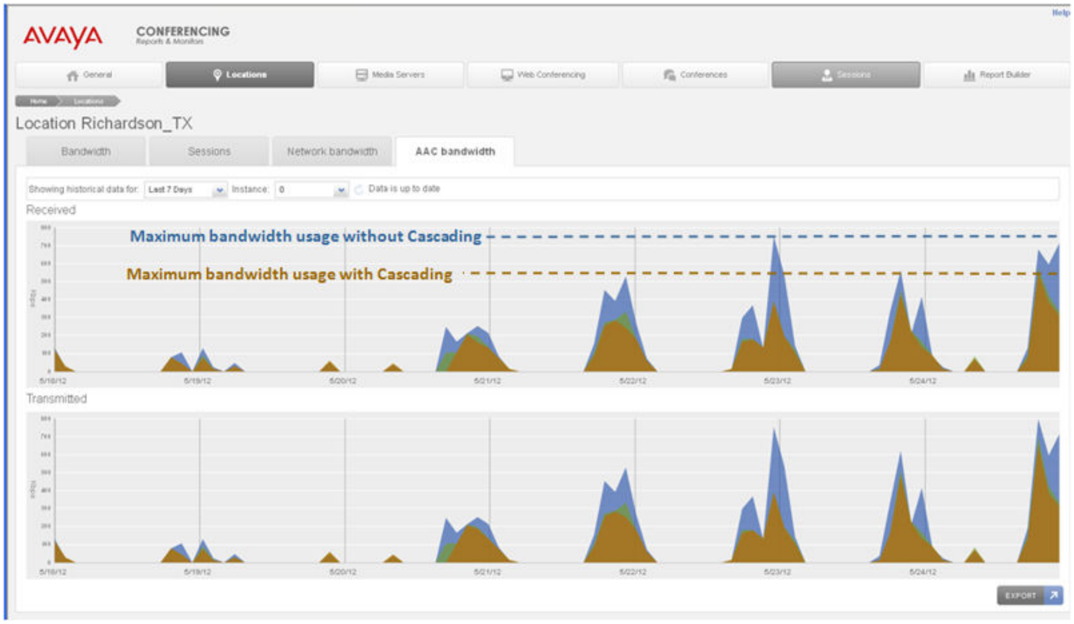
## Monitoring bandwidth usage

If the communications patterns are uncertain prior to the introduction of Avaya Aura® Conferencing, bandwidth and port usage can be monitored closely during a phased rollout of the service to ensure that bandwidth usage is occurring as expected.

Key performance indicators (KPI) are provided by the Avaya Aura® Conferencing management tools, including information on bandwidth usage. The following data is reported on an individual location basis:

- Requested bandwidth: The bandwidth that is required without media cascading
- Negotiated bandwidth: The bandwidth that is required after media cascading is applied
- Actual bandwidth: A real time measurement of bandwidth usage, as measured by the Avaya Aura® Media Server. This can be used to determine whether there is a gap between the bandwidth requested within SIP signaling and bandwidth that is actually consumed.

The following figure shows one of the reports available in the Element Manager monitoring reporting tools to monitor usage patterns for a location. This report also shows an example of optimization that can be provided by media cascading by comparing the peak requested bandwidth with the peak negotiated bandwidth for a location. Bandwidth savings depends on a number of factors that can be unique to a location.



Location Richardson_TX

Showing historical data for: Last 7 Days

Instance: 0

Data is up to date

**Figure 16: Location report — AAC bandwidth**

## Related links

Shared bandwidth management on page 79

# Chapter 4: Before you begin

## Before you begin checklist

The following checklist provides the high level steps and considerations prior to beginning your Avaya Aura® Conferencing installation. This checklist applies to deployments which use the Avaya Aura® environment, which consists of System Manager and Session Manager. If you wish to install Avaya Aura® Conferencing in an alternative environment, you can proceed directly to the next chapter. An installation of Avaya Aura® Conferencing in an alternative environment is called Avaya Aura® Conferencing Turnkey solution.

**Note:**

If you are upgrading from Avaya Aura® Conferencing Release 7.2, see Upgrading Avaya Aura® Conferencing, which is available from http://support.avaya.com/.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Ensure that version 6.2 is installed for System Manager, Session Manager, and Communication Manager prior to installing Avaya Aura® Conferencing. Obtain the System Manager IP address and FQDN. | For more information about the supported versions of the Avaya Aura® stack, see the *Overview and Specification Guide for Avaya Aura® Conferencing*, which is available from http://support.avaya.com/. To learn more about alternative platform software solutions, see the *Overview and Specification Guide for Avaya Aura® Conferencing Turnkey Solution*, which is also available from http://support.avaya.com/ | | |
| 2 | Ensure that the **Ignore SDP for Call Admission Control** setting is disabled in System Manager.<br>**Important:**<br>The **Ignore SDP for Call Admission Control** setting in System Manager | Perform the following steps:<br>1. Log on to System Manager.<br>2. On the System Manager console, click **Session Manager** in the Elements section.<br>3. In the left navigation pane, click **Session Manager Administration**.<br>4. In the Global Settings section on the Session Manager Administration page, make sure the **Ignore SDP for** | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| | *must be* disabled for Avaya Aura® Conferencing to operate properly. | **Call Admission Control** check box is not checked.<br>5. If you changed the **Ignore SDP for Call Admission Control** setting, click **Save**. | | |
| 3 | Download the Avaya Aura® Conferencing Intelligent Workbook from the Avaya Web site. | Go to http://support.avaya.com/ to download the Avaya Aura® Conferencing Intelligent Workbook. | | |
| 4 | Determine your deployment layout type based on the capacity and scaling requirements for your location. | Include this information in the Avaya Aura® Conferencing Intelligent Workbook<br>For information about deployment types, see the various Overview and Specification Guides and the Solution Description Guides in Documentation on page 20. | | |
| 5 | Obtain the CD-ROM disk with latest Common Server 3.0 BIOS settings tool. | CD-ROM disk is provided | | |
| 6 | Install your HP ProLiant DL360 G9 server. | See HP Server overview on page 85. | | |
| 7 | Obtain the latest Avaya Aura® Conferencing disks for software installation and patches:<br>• AAC platform DVD-ROM<br>• Application Bundle DVD-ROM<br>• Platform patches DVD-ROM | DVD-ROM disks are provided. You can also download from Avaya PLDS and burn your own CD- or DVD-ROM (for advanced users only). | | |
| 8 | Use the Avaya Aura® Conferencing Intelligent Workbook for the following:<br>• Determine the required number of IP addresses for your deployment | See the Avaya Aura® Conferencing Intelligent Workbook you previously downloaded. | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| | configuration, hostnames, and FQDNs.<br>- Register the required FQDNs with the appropriate DNS servers.<br>**Important:**<br>FQDNs are required for single sign-on (SSO) to enable you to administer all the components using System Manager. DNS integration is required for SSO to work.<br>**Note:**<br>To use SSO, the System Manager FQDN, Element Manager FQDN, and Provisioning Client FQDN (if required) must belong to the same root domain. | | | |
| 9 | Obtain an enrollment password from System Manager. | See Obtaining enrollment password from System Manager on page 564. | | |
| 10 | If you are deploying your system with TLS enabled, ensure Certificate Authorities are imported and certificates are assigned. | See Introduction to certificates on page 552. | | |
| 11 | Obtain the supported Web browsers. | Check the latest Avaya Aura® Conferencing Release Notes which are available from http://support.avaya.com/ to see the exact versions of the Web | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| | | browsers which Avaya Aura® Conferencing supports. | | |
| 12 | Obtain the License key file from Avaya and install the key on the WebLM server which resides on System Manager. | See Installing the license key on page 171. | | |
| 13 | If you are using a DMZ deployment, consider the following:<br>• Ensure you have configured the required servers, routers, and firewalls.<br>• Ensure the required port modifications are made. | Contact your network specialist or administrator if you have a large deployment with redundancy or a large simplex deployment and require a DMZ configuration.<br>For more information, see Enterprise DMZ deployment on page 45.<br>For the complete *Port Matrix: Avaya Aura® Conferencing* document, go to http://support.avaya.com. | | |

# Chapter 5: Installing hardware for Avaya Aura® and Turnkey deployments

## Avaya Aura® and Turnkey deployments

The hardware requirements for Avaya Aura® Conferencing are the same whether you are installing the product in an Avaya Aura® deployment or a Turnkey deployment. In both cases, it is the HP ProLiant DL360 G9 server.

## Installing the HP ProLiant DL360 G9 Server

### HP Server overview

The Avaya Common Servers category includes HP servers that support several Avaya software solutions, some requiring more hardware, and memory requirements beyond the standard configuration. This document covers the standard configuration only—consult specific Avaya product documentation for application-specific or solution-specific server configurations.

- Avaya Common Servers are supplied under an OEM relationship and Avaya servers are treated differently than other commercially available servers from the vendors.
- Avaya Common Servers are turnkey appliances. No server designed for a particular application can be repurposed for use with another application. The only exception to this is when an application has provided an upgrade or migration path from one server state to a different server state with the appropriate kits, tools, documentation, and training materials. For example, System Platform is providing a kit plus documentation for migrating a server running System Platform to Appliance Virtualization Platform.
- Neither customers, business partners, distributors, nor Avaya Associates interacting with customers and business partners, should get BIOS or other firmware updates for any third-party OEM servers forming part of Avaya's turnkey appliance offers. Only consult Avaya-provided downloads, information and support. All BIOS or firmware updates are provided through Avaya. Go to the Avaya Support website at http://support.avaya.com for additional information.
- Remote access and use of HP iLO hardware management tools for the HP servers are employed by a limited number of Avaya applications. If HP iLO is supported, that

application's documentation will define its configuration and use. Please check with the Avaya application product manager or appropriate documentation to confirm support.

- Do not contact HP for Service; all support, warranty, repair, and maintenance are through the Avaya processes. If the server is purchased from Avaya, customer first point of contact is Avaya to troubleshoot hardware issues.

  Service and repair of consumable accessories and cables are not covered under maintenance. Customers must purchase these items.
- Avaya strongly recommends that all servers are protected with an Uninterruptable Power Supply for power surge and interruption protection. Avaya is not responsible for servers damaged by power surges, brown outs, black outs etc.
- Substitution of a DC power supply for a server must be approved by the Application Product Manager before substitution. If there is a significant demand for a turnkey solution with a DC power supply, an Avaya GRIP (Global Requirements Integration Process) request must be submitted. Partners registered to use this process can submit a GRIP request at https://portal.avaya.com/apps/grip/partner.asp. Avaya Associates may assist and can find information about this process at http://spark4.avaya.com/grip. Note, a GRIP request must be made for the Avaya application product, not the server model. The decision on whether to include a turnkey offer with a DC power supply is the responsibility of each Avaya application Product Manager. The name of the Product Managers for each application is at the bottom of the application page on the Avaya Global Sales portal.
- Product labels on the servers themselves have the 9-digit base server codes and a base server description for Avaya Services in service and support. These 9-digit codes differ from the 6-digit orderable codes under which servers are ordered. On every server package, there is a Packing Label and a Hierarchy Label. The Hierarchy Label itemizes the stock list in the box of the 6-digit orderable code and Avaya recommends retaining them for reference.
- Quality assurance – product integrity testing and environmental international restrictions were completed by HP and verified with Avaya using Design for Environmental Checklists. The list includes: batteries, printed wiring boards, plastic parts, product packaging, RoHS, green requirements, and energy efficiency.

**Related links**

Registration on page 86

## Registration

- Registration is mandatory to receive support from Avaya, as described in the Avaya's SFAP or SAP policy. Avaya SFAP policy is available at http://support.avaya.com https://downloads.avaya.com/css/P8/documents/100075395. Also, you can go to the Avaya Support website at http://support.avaya.com under **Help & Policies** > **Policies & Legal** > **Intellectual Property Policy**.
- Avaya direct customers and Global Business Partners registration must go through the Global Registration Tool (GRT) process through http://support.avaya.com, directly accessed by: https://grt.avaya.com/grt/ **- Create A New Registration**.

**Related links**

HP Server overview on page 85

## How to use this document

This guide contains information for installing the server as part of an Avaya deployment and provides:

- Instructions for how to find the appropriate online server documentation from HP.
- References to specific topics in standard HP documentation
- Suggested changes, details, and notes to assist the user in interpreting the manufacturer's documentation and to clarify Avaya's recommended implementation of the equipment
- Topics not covered in standard HP documentation, but which are necessary for successful installation and maintenance of Avaya products

## Downloading HP documentation

Use this procedure to find and download the server documentation.

### Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter Your Product Here** search box, type `Common Servers` and then select 3.0.x from the drop-down list.

   If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
6. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
7. Click **Enter**.

## HP ProLiant DL360 G9 document set

### Documents

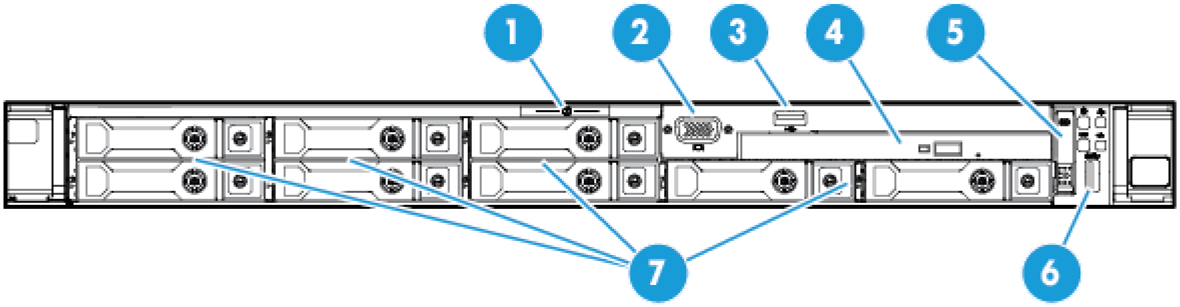
- HP ProLiant DL360 G9 Server User Guide
- HP ProLiant DL360 G9 Server Maintenance and Service Guide
- HP ProLiant DL360 G9 Troubleshooting Guide, Volume I: Troubleshooting

- HP ProLiant DL360 G9 Troubleshooting Guide, Volume II: Error Messages
- HP Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products

### Documents included in the shipping container

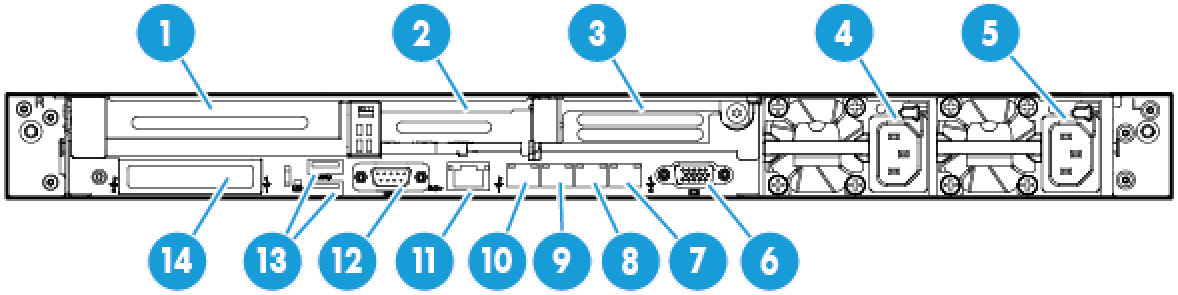
| Title | Part number |
|---|---|
| Safety, Compliance, and Warranty Information | 703828 - 023 |
| Quick Deploy Rail System Installation Instructions (located in rail kit box) | 740122-002 |

## Front view of HP ProLiant DL360 G9 Server



| No. | Description |
|---|---|
| 1 | Serial label pull tab |
| 2 | Front video connector |
| 3 | USB 2.0 connector |
| 4 | Optical drive |
| 5 | Systems Insight Display (Not used in Avaya configurations) |
| 6 | USB 3.0 connector |
| 7 | Hard Drive bays*<br>* The HDDs read starting with top left, then bottom left, and continues to the right. |

## Rear view of HP ProLiant DL360 G9 Server



| No. | Description |
|---|---|
| 1 | Slot 1 PCIe3 x16 (16, 8, 4, 1) |
| 2 | Slot 2 PCIe 3 x8 (8, 4, 1) |
| 3 | Slot 3 PCIe 3 x16 (16, 8, 4, 1) (Not used in Avaya configurations) |
| 4 | Power supply 2 |
| 5 | Power supply 1 |
| 6 | Video connector |
| 7 | NIC connector 4 |
| 8 | NIC connector 3 |
| 9 | NIC connector 2 |
| 10 | NIC connector 1 |
| 11 | iLO 4 connector |
| 12 | Serial connector |
| 13 | USB 3.0 connectors |
| 14 | FlexibleLOM bay (Not used in Avaya configurations) |

## HP ProLiant DL360 G9 Server specifications

| Base unit | Baseline | Options |
|---|---|---|
| DL360 G9 | 1U Chassis, Dual Socket | DL380p G9 2U Chassis, Dual Socket |
| Processor | Intel E5-2620v3, Six Core 2.3 GHz (Haswell)<br>4 memory channels per CPU with up to 3 DIMMs per channel (most applications use 1 or 2 DIMMs per channel to optimize memory speed) | • Intel E5–2640v3 Eight Core/2.6 GHz (Haswell)<br>• Intel E5–2680v3 Twelve Core/2.5 GHz (Haswell) |

*Table continues…*

| Base unit | Baseline | Options |
|---|---|---|
| Memory | 4 GB DDR4 RDIMMs | Max Capacity for memory (4 GB RDIMM):<br>• 48 GB, 12 x 4 GB (1 proc)<br>• 96 GB, 24 x 4 GB (2 proc) |
| HW RAID | P440ar RAID controller with 2 GB Cache and battery backup. Optioned as RAID 1, 5, or 10. | Other RAID configurations available |
| Hot-Plug disk drive cage | 8 Small Form Factor 2.5” hot-plug hard drive bays are available when an optical drive is installed. | N/A |
| Disk drive | 300 GB SAS 2.5" 10K RPM 6G DP Hard Drive. Two base configurations:<br>• 279 GiB total: RAID 1, 2 x 300 GB drives<br>• 559 GiB total: RAID 5, 3 x 300 GB drives<br>• 838 GiB total: RAID 5, 4 x 300 GB drives<br>• 559 GiB total: RAID 10, 4 x 300 GB drives<br>**Note:**<br>• 1 GB = $10^9$ Bytes<br>• 1 GiB = $2^{30}$ Bytes | • Additional 300 GB 10K RPM SAS drive<br>• High performance 300 GB 15K SAS drives<br>• High capacity 600 GB 10K SAS drives<br>• High performance 900 GB 10K SAS drives<br>• High capacity 1.2 TB 10K SAS drives<br>**Note:**<br>For each application, the system displays the hard drive capacities that are specified for the application. |
| NICs | 4 or 6 integrated ENET Gigabit NIC ports with TCP offload engine (included on motherboard) | Two additional dual NIC slots may be populated for certain applications. |
| PCIe slots | Three PCI-Express Gen 3 expansion slots: (1) full-height, 3/4-length slot and (1) low-profile slots | Slot 1 is full height / 3/4-length x16<br>Slot 1 is low profile / half length x8 |
| Removable media | Slim line SATA DVD-RW optical drive (used in all Avaya configurations) | No additional options supported. |
| Power supply | 500 W or 800 W hotplug AC power supply | • 800 W DC power supply<br>• Single and dual power supply configurations |
| Fans | 5 Fan modules in 1 processor model | 7 fan modules hot-swappable (fan redundancy standard) |
| Additional items | 2 front USB (1–2.0, 1–3.0), 2 back USB (3.0), 1 internal USB port, and front video connector | |

## Altitude and air pressure requirements

The following table lists the altitude and air pressure requirements for the server.

| Specification | Value |
|---|---|
| Operating | 3050 m (10,000 ft). This value may be limited by the type and number of options installed. Maximum allowable altitude change rate is 457 m/min (1500 ft/min). |
| Non-operating | 9144 m (30,000 ft). Maximum allowable altitude change rate is 457 m/min (1500 ft/min). |

## Hardware dimensions and clearance requirements

The following table lists the dimensions and clearance requirements for the server.

| Type | Description |
|---|---|
| Dimensions | Height: 4.29 cm (1.69 in) |
| | Width: 43.46 cm (17.11 in) |
| | Depth: 69.90 cm (27.50 in) |
| Weight (maximum: 10 drives, two processors, two power supplies, two heatsinks, one Smart Array controller, seven fans) | 15.31 kg (33.36 lb) |

## Temperature and humidity requirements

The following table lists the temperature and humidity requirements for the server.

| Specification | Value |
|---|---|
| Temperature range | **Note:**<br>All temperature ratings shown are for sea level. An altitude derating of 1°C per 304.8 m (1.8° per 1,000 ft.) above sea level to a maximum of 3048 m (10,000 ft), no direct sustained sunlight. |
| Operating | 10° to 35°C (50° to 95°F) Maximum rate of change is 20°C/hr (36°F/hr). The upper limit might be limited by the type and number of options installed. System performance may be reduced if operating with a fan fault or above 30°C (86°F). |
| Non-operating | -30° to 60°C (-22° to 140°F). Maximum rate of change is 20°C/hr (36°F/hr). |

*Table continues…*

| Specification | Value |
|---|---|
| Relative humidity (non-condensing) | |
| Operating | 8 to 90% relative humidity (Rh), 24°C (75.2°F) maximum wet bulb temperature, non-condensing. |
| Non-operating | 5 to 95% relative humidity (Rh), 38.7°C (101.7°F) maximum wet bulb temperature, non-condensing. |

## Power requirements

The following table lists the power requirements for the server.

**Table 9: HP 800 W CS power supply (92% efficiency)**

| Specification | Value |
|---|---|
| BTU | 917 BTU/hr |
| Voltage | 100V — 240V |
| Plug Type | NEMA — 15 |
| Circuit Breaker | 15 Amp |
| Pole | 1 |
| AMP Draw | 2.7 @ 100VAC |
| Total Watts | 269 W |

**Note:**

These numbers are based on the following typical Avaya configuration:

- qty=2 – E5-2620v3 six core processors
- qty=8x4 GB – Memory (1Rx4 PC4-2133P –R Kit)
- qty=3 – 2.5” SFF SAS HDDs
- qty=1 – Ethernet 1Gb 2-port 332T adaptor
- qty=2 – 800W power supplies

## Physical system protection requirements

To properly ventilate the system, you must provide a minimum clearance of:

- 63.5 cm (25 in) in front of the rack
- 76.2 cm (30 in) behind the rack

**Note:**

You must ensure that no environmental hazards, such as, excessive heat, excessive humidity, improper ventilation, or electromagnetic interference from proximate equipment interfere with the operation of the server.

## Checklist for installing the server in the rack

This installation checklist contains the principle steps that are necessary to install the server in the rack. The notation in the *Reference* column is a section in the appropriate HP document that contains the step-by-step procedures. Where applicable, additional information and clarifications appear in the *Avaya recommendation* column. Perform each task in the order specified.

**Note:**

Avaya customers are required to have a monitor and USB keyboard available for server maintenance.

| No. | Task | Reference | Avaya recommendation |
|---|---|---|---|
| 1 | Observe safety warnings. | User Guide: Installing the server into the rack. | |
| 2 | Examine contents of shipping container (Avaya provided equipment). | User Guide: Identifying the contents of the server shipping carton | • Server<br>• Rail Kit<br>• Printed setup documentation<br>• Rack mounting hardware kit and documentation |
| 3 | Examine installation environment (customer provided equipment). | User Guide: Optimum Environment | When installing the server in a rack, select a location that meets the environmental standards. |
| 4 | Verify that the rack is installed according to the manufacturer's instructions and in accordance with all local codes and laws. | User Guide: Installing the server into the rack | To install the server into a rack with square, round, or threaded holes, refer to the instructions that ship with the rack hardware kit. |
| 5 | Verify that the rack is grounded in accordance | User Guide: Electrical grounding requirements | The server must be grounded for proper operation and safety. |

*Table continues…*

| No. | Task | Reference | Avaya recommendation |
|---|---|---|---|
| | with local electrical code. | | |
| 6 | Determine and plan the vertical spacing of the servers in the frame. | User Guide: Space and Airflow Requirements | Servers draw in cool air through the front and expel warm air through the rear. Therefore, the front rack doors must be adequately ventilated to allow ambient room air to enter the cabinet, and the rear door must be adequately ventilated to allow the warm air to escape from the cabinet. |
| 7 | Attach the rails to the rack. | User Guide: Installing the server into the rack | To install the server into a rack with square, round, or threaded holes, refer to the instructions that ship with the rack hardware kit. If these rails do not fit the rack the customer must provide rails or a shelf for rack installation. Also the rails included with the server might not work with round hole racks, in which case the customer can obtain rails and/or a shelf from a distributor. (RackSolutions.com) |
| 8 | Attach the server to the rack. | User Guide: Installing the server into the rack | ⚠ **Warning:**<br>This server is very heavy. To reduce the risk of personal injury or damage to the equipment:<br>• Get help lifting and stabilizing the product during installation or removal, especially when the product is not fastened to the rails. HP recommends that a minimum of two people are required for all rack server installations. A third person may be required to help align the server if the server is installed higher than chest level.<br>• Use caution when installing the server in or removing the server from the rack; it is unstable when not fastened to the rails. |
| 9 | Connect the peripheral devices to the server. | User Guide: Setup<br>• Connecting peripheral devices to the server<br>• Connecting the power cord to the power supply | Network connections, power cords<br>See Avaya application installation documentation. |
| 10 | Power up the server. | User Guide: Power up the server | Once the server is powered on, see Avaya application installation instructions.<br>Server comes pre-installed with Avaya approved firmware, settings and RAID configuration. Do not go to the HP website for any updates unless instructed by Avaya. |

## Setting an administrator password

### About this task

You can set a password to protect the server from changes to the BIOS settings. In addition, the password protects against configuration changes such as updates to the Boot order, iLO configuration, and Boot enable or disable.

If you add password for BIOS, you must protect, retain, and provide the password when changes to the server are required.

### Before you begin

Ensure that a monitor and USB keyboard are connected to the server.

### Procedure

1. While restarting or turning on the server, at the HP splash screen press `F9` to select **System Utilities**.
2. Select **System Configuration** > **BIOS Platform Configuration (RBSU)** > **Server Security**.
3. Move the cursor to the **Set Admin Password** field, and press `Enter`.
4. Type a password and press `Enter`.

   The system displays a message to confirm the password.
5. Press `Esc` to go back to **System Utilities** in the menu.
6. Press `Enter` to exit.

## Updating the HP ProLiant DL360 G9 server power management settings

Use this procedure to update the BIOS of the HP ProLiant DL360 G9 server to enable its maximum performance mode of operation. Maximum performance mode provides the best real-time performance option for the server.

**Note:**

Running the HP ProLiant DL360 G9 server in maximum performance mode places the highest requirements on power usage by the server. Consult the HP ProLiant DL360 G9 server documentation for maximum power requirements and ensure the power circuit hosting this server has adequate amperage to supply this server and all other servers that share the circuit.

## Before you begin

You must have CD-ROM disk with latest Common Server 3.0 BIOS settings tool.

## Procedure

1. On the HP ProLiant DL360 G9 server, insert the Common Server 3.0 BIOS settings tool CD into the CD-ROM drive.
2. Boot the system from the Common Server 3.0 BIOS settings tool CD.
3. When prompted, press any key to read the EULA or press space bar to view the EULA in page mode.
4. At the **Do you accept the terms of this EULA? (Y)es/(No):** prompt, type **Y** and press **Enter**.
5. When prompted, type **Y** to indicate that you are ready to start running the tool.

   The BIOS UEFI mode is disabled and system is rebooted.
6. Leave the disk in the CD-ROM drive.
7. Boot the system again from the Common Server 3.0 BIOS settings tool CD.
8. When prompted, press any key to read the EULA or press space bar to view the EULA in page mode.
9. At the **Do you accept the terms of this EULA? (Y)es/(No):** prompt, type **Y** and press **Enter**.
10. When prompted, type **Y** to indicate that you are ready to start running the tool.

    When the final check to verify the Legacy Boot Mode is completed successfully, the Common Server 3.0 BIOS settings tool CD is ejected and system is rebooted.

# Chapter 6: Managing HP smart arrays

## Managing Hewlett Packard™ Smart Arrays

This section describes how to configure the Avaya Aura® Conferencing hard drives to RAID array(s) on the HP ProLiant DL360 G9 hardware for the different types of servers used by Avaya Aura® Conferencing, such as recording servers and cascading servers. Avaya recommends that you use the HP DL360 G9/HP DL380 G9 RAID Configuration Tool to configure the Avaya Aura® Conferencing hard drives. If the HP DL360 G9/HP DL380 G9 RAID Configuration Tool is not available, you can use the HPSSA tool.

You can obtain the HP DL360 G9/HP DL380 G9 RAID Configuration Tool from Avaya PLDS (Product Licensing and Delivery System).

Hewlett Packard™ Smart Storage Administrator (HPSSA) is a single interface that sets up, configures, and manages the HP Smart Arrays controllers and the HP SAS Host Bus Adapters (HBA).

**Related links**

Using the HP DL360 G9/HP DL380 G9 RAID Configuration Tool on page 97

Using the HPSSA tool on page 99

## Using the HP DL360 G9/HP DL380 G9 RAID Configuration Tool

Avaya provides a HP DL360 G9/HP DL380 G9 RAID Configuration Tool to help you to configure the RAID arrays.

**Related links**

Configuring or clearing the RAID 10 array for non-recording servers using the HP DL360 G9/HP DL380 G9 RAID Configuration Tool on page 98

Configuring or clearing the RAID 1 array for cascading servers using the HP DL360 G9/HP DL380 G9 RAID Configuration Tool on page 99

# Configuring or clearing the RAID 10 array for non-recording servers using the HP DL360 G9/HP DL380 G9 RAID Configuration Tool

### Before you begin

Ensure that:

- You have a keyboard, mouse, and monitor.
- You have backed up any important data.
- You have the HP DL360 G9/HP DL380 G9 RAID Configuration Tool.
- You have installed the 4 x 300 GB hard drives in bays 1–4.

**Note:**

Do not remove hard disk drives while the tool is executing.

### About this task

Use this procedure to configure the two hard drives to one RAID 1 array on the HP ProLiant DL360 G9 cascading servers.

### Procedure

1. On the HP ProLiant DL360 G9 server, insert the HP DL360 G9/HP DL380 G9 RAID Configuration Tool into the CD-ROM drive.
2. Boot the system from the HP DL360 G9/HP DL380 G9 RAID Configuration Tool.
3. When prompted by the license agreement (EULA), press the space button to read it. Continue to press space to read the text to the end.
4. When prompted, accept the license agreement by typing `Y`.
5. When prompted, type `Y` to continue running the tool.
6. Type `Y` to delete all data and RAID arrays or type `N to` preserve the data.
7. At the **What type of Array do you want to create? RAID 5 or RAID 10 (5/10)?** prompt, type `10` and press `Enter`.

   The tool loads the Avaya Aura® Conferencing RAID settings, ejects the disk, and powers off the server. The RAID settings are successfully configured.
8. Eject the HP DL360 G9/HP DL380 G9 RAID Configuration Tool.

**Related links**

Using the HP DL360 G9/HP DL380 G9 RAID Configuration Tool on page 97

## Configuring or clearing the RAID 1 array for cascading servers using the HP DL360 G9/HP DL380 G9 RAID Configuration Tool

### Before you begin

Ensure that:

- You have a keyboard, mouse, and monitor.
- You have backed up any important data.
- You have the HP DL360 G9/HP DL380 G9 RAID Configuration Tool.
- You have installed the 2 x 300 GB hard drives in bays 1–2.

**Note:**

Do not remove hard disk drives while the tool is executing.

### About this task

Use this procedure to configure the two hard drives to one RAID 1 array on the HP ProLiant DL360 G9 cascading servers.

### Procedure

1. On the HP ProLiant DL360 G9 server, insert the HP DL360 G9/HP DL380 G9 RAID Configuration Tool into the CD-ROM drive.
2. Boot the system from the HP DL360 G9/HP DL380 G9 RAID Configuration Tool.
3. When prompted by the license agreement (EULA), press the space button to read it. Continue to press space to read the text to the end.
4. When prompted, accept the license agreement by typing `Y`.
5. When prompted, type `Y` to continue running the tool.
6. Type `Y` to delete all data and RAID arrays or type `N` to preserve the data.

   The tool loads the Avaya Aura® Conferencing RAID settings, ejects the disk, and powers off the server. The RAID settings are successfully configured.
7. Eject the HP DL360 G9/HP DL380 G9 RAID Configuration Tool.

**Related links**

Using the HP DL360 G9/HP DL380 G9 RAID Configuration Tool on page 97

# Using the HPSSA tool

Avaya recommends that you use the HP DL360 G9/HP DL380 G9 RAID Configuration Tool to configure the Avaya Aura® Conferencing hard drives. If the HP DL360 G9/HP DL380 G9 RAID Configuration Tool is not available, you can use the HPSSA tool.

**Related links**

Launching the Hewlett Packard Smart Storage Administrator (HPSSA) tool on page 100
Exiting from the Hewlett Packard Smart Storage Administrator (HPSSA) tool on page 101
Configuring the RAID arrays for non-recording servers using the HPSSA tool on page 102
Configuring the RAID arrays for recording servers using the HPSSA tool on page 103
Configuring the RAID arrays for cascading servers using the HPSSA tool on page 105
Clearing the RAID arrays for non-recording servers using the HPSSA tool on page 106
Clearing the RAID arrays for recording servers using the HPSSA tool on page 107
Clearing the RAID arrays for cascading servers using the HPSSA tool on page 108

# Launching the Hewlett Packard™ Smart Storage Administrator (HPSSA) tool

## Before you begin

Ensure that:

- You have a keyboard, mouse, and monitor.
- You have backed up any important data.

**Note:**

Do not remove hard disk drives while the tool is executing.

## About this task

Use this task to launch HPSSA. HPSSA is the tool that you require in order to configure or reconfigure RAID 10 array(s) on the HP ProLiant DL360 G9 server

## Procedure

1. Turn on or reboot the HP ProLiant DL360 G9 server.
2. During server boot, wait until you see **F9 System Utilities** displayed in the bottom left corner.
3. Press `F9`.

   The **System Utilities** menu is displayed.
4. Select **System Configuration** from the menu and press `Enter`.
5. Select **Embedded RAID: Smart Array P440ar Controller** from the menu and press `Enter`.

   The **Smart Array P440ar Controller** menu is displayed.
6. Select **Exit and launch HP Smart Storage Administrator (HPSSA)** from the menu and press `Enter`.

   The system starts HPSSA mode. It may take a few minutes to fully boot.

7. In HPSSA mode, from the **Array Controller(s)** section of the left panel menu, select **Smart Array P440ar**.

   The **Smart Array P440ar** page is displayed in the right panel.

8. From the right panel, select **Configure** and press `Enter`.

   The **RAID Array(s) configuration** page is displayed.

**Related links**

Using the HPSSA tool on page 99

## Exiting from the Hewlett Packard™ Smart Storage Administrator (HPSSA) tool

### Before you begin

Ensure that:

- You have a keyboard, mouse, and monitor.
- You have backed up any important data.

**Note:**

Do not remove hard disk drives while the tool is executing.

### About this task

Use this task to exit from the HPSSA tool and to apply all configuration changes to the RAID arrays.

### Procedure

1. Click the **X** close button in the upper right corner.

   A confirmation dialog is displayed.

2. Click **OK** on the confirmation dialog.
3. Click the ⏻ button in the upper right corner.

   A confirmation dialog is displayed.

4. Click the ↻ button to reboot the server or click the ⏻ button to shut down the server.

**Related links**

Using the HPSSA tool on page 99

# Configuring the RAID arrays for non-recording servers using the HPSSA tool

## Before you begin

Ensure that:

- You have a keyboard, mouse, and monitor.
- You have backed up any important data.
- You have launched the HPSSA tool.
- You have installed the 4 x 300 GB hard drives for all core servers.

✱ **Note:**

Do not remove hard disk drives while the tool is executing.

## About this task

Use this procedure to configure the four hard drives to one RAID 10 array on the HP ProLiant DL360 G9 non-recording core servers.

## Procedure

1. Check for any unassigned drives on the left panel: In the **Controller Devices** sub-menu, look at the text under the **Unassigned Drives** menu.

   If there are no unassigned drives, you can:

   - Reconfigure the RAID arrays using the HPSSA tool if you want to change the configuration.
   - Exit from the HPSSA tool if you are satisfied with the configuration.
2. In the **Controller Devices** sub-menu, click **Logical Devices** to check if the information listed is correct.
3. Check for any unassigned drives on the left panel: In the **Controller Devices** sub-menu, look at the text under the **Unassigned Drives** menu.

   There should be four 300GB drives in bays 1- 4.
4. Select the drives in bays 1 to 4 and click the **Create Array** button and in the Create Logical Drive window, perform the following actions:

| Choice Option | Choice Description |
|---|---|
| **RAID Level** | Select **RAID 1+0**. |
| **Strip Size/Full Stripe Size** | Select **256 KiB/512 KiB**. |
| **Sectors/Track** | Select **32**. |
| **Size** | Select **Maximum Size: 572140 MiB (558.7 GiB)**. |
| **Caching** | Select **Enabled**. |

5. Click the **Create Logical Drive** button.
6. On the results window, click the **Finish** button.
7. Check for any unassigned drives on the left panel: In the **Controller Devices** sub-menu, look at the text under the **Unassigned Drives** menu.

   If there are unassigned devices, check that you have followed the steps correctly. If there are no unassigned devices, you can exit the tool or use it to make any changes to the configuration that you require.

**Related links**

Using the HPSSA tool on page 99

## Configuring the RAID arrays for recording servers using the HPSSA tool

### Before you begin

Ensure that:

- You have a keyboard, mouse, and monitor.
- You have backed up any important data.
- You have launched the HPSSA tool.
- You have installed the 4 x 300 GB hard drives for all core servers.
- You have installed the 4 x 900 GB hard drives from the Avaya Aura® Conferencing upgrade kit for recording servers.

**Note:**

Do not remove hard disk drives while the tool is executing.

### About this task

Use this procedure to configure the eight hard drives to two RAID 10 arrays on the HP ProLiant DL360 G9 recording servers.

### Procedure

1. Check for any unassigned drives on the left panel: In the **Controller Devices** sub-menu, look at the text under the **Unassigned Drives** menu.

   If there are no unassigned drives, you can:

   - Reconfigure the RAID arrays using the HPSSA tool if you want to change the configuration.
   - Exit from the HPSSA tool if you are satisfied with the configuration.
2. In the **Controller Devices** sub-menu, click **Logical Devices** to check if the information listed is correct.

3. Check for any unassigned drives on the left panel: In the **Controller Devices** sub-menu, look at the text under the **Unassigned Drives** menu.
    - If RAID array is not configured for drives in bays 1-4, there should be four 300GB drives.
    - If RAID array is not configured for drives in bays 5-8, there should be four 900GB drives.

If RAID array is not configured for drives in bays 1-4, perform the following actions:

4. Select the drives in bays 1 to 4 and click the **Create Array** button and in the Create Logical Drive window, perform the following actions:

| Choice Option | Choice Description |
|---|---|
| **RAID Level** | Select **RAID 1+0**. |
| **Strip Size/Full Stripe Size** | Select **256 KiB/512 KiB**. |
| **Sectors/Track** | Select **32**. |
| **Size** | Select **Maximum Size: 572140 MiB (558.7 GiB)**. |
| **Caching** | Select **Enabled**. |

If RAID array is not configured for drives in bays 5-8, perform the following actions:

5. Select the drives in bays 5 to 8 and click the **Create Array** button and in the Create Logical Drive window, perform the following actions:

| Choice Option | Choice Description |
|---|---|
| **RAID Level** | Select **RAID 1+0**. |
| **Strip Size/Full Stripe Size** | Select **256 KiB/512 KiB**. |
| **Sectors/Track** | Select **32**. |
| **Size** | Select **Maximum Size: 1716902 MiB (1.6 TiB)**. |
| **Caching** | Select **Enabled**. |

6. Click the **Create Logical Drive** button.
7. On the results window, click the **Finish** button.
8. Check that the RAID arrays are configured correctly.
    a. In the **Controller Devices** sub-menu, click the **Physical Devices** menu.

       In the central panel, information is displayed about RAID arrays A and B.

    b. Check that the size of RAID array A (RAID 1+0) is 599.93GB and the size of RAID array B (RAID 1+0) is 1.80TB.

    c. If the information is not correct, reconfigure the RAID arrays using the HPSSA tool.
9. Check for any unassigned drives on the left panel: In the **Controller Devices** sub-menu, look at the text under the **Unassigned Drives** menu.

   If there are unassigned devices, check that you have followed the steps correctly. If there are no unassigned devices, you can exit the tool or use it to make any changes to the configuration that you require.

**Related links**

Using the HPSSA tool on page 99

## Configuring the RAID arrays for cascading servers using the HPSSA tool

### Before you begin

Ensure that:

- You have a keyboard, mouse, and monitor.
- You have backed up any important data.
- You have launched the HPSSA tool.
- You have installed the 2 x 300 GB hard drives for all cascading servers.

✱ **Note:**

Do not remove hard disk drives while the tool is executing.

### About this task

Use this procedure to configure the two hard drives to one RAID 1 array on the HP ProLiant DL360 G9 cascading servers.

### Procedure

1. Check for any unassigned drives on the left panel: In the **Controller Devices** sub-menu, look at the text under the **Unassigned Drives** menu.

   If there are no unassigned drives, you can:

   - Reconfigure the RAID arrays using the HPSSA tool if you want to change the configuration.
   - Exit from the HPSSA tool if you are satisfied with the configuration.
2. In the **Controller Devices** sub-menu, click **Logical Devices** to check if the information listed is correct.
3. Click the **Create Array** button.

   There should be two 300GB drives in bays 1 and 2.
4. Select the drives in bays 1 and 2 and click the **Create Array** button.
5. In the Create Logical Drive window, perform the following actions:

| Choice Option | Choice Description |
|---|---|
| **RAID Level** | Select **RAID 1**. |
| **Strip Size/Full Stripe Size** | Select **256 KiB/256 KiB**. |
| **Sectors/Track** | Select **32**. |

| Choice Option | Choice Description |
|---|---|
| **Size** | Select **Maximum Size: 286070 MiB (279.3 GiB)**. |
| **Caching** | Select **Enabled**. |

6. Click the **Create Logical Drive** button.
7. On the results window, click the **Finish** button.
8. Check for any unassigned drives on the left panel: In the **Controller Devices** sub-menu, look at the text under the **Unassigned Drives** menu.

   If there are unassigned devices, check that you have followed the steps correctly. If there are no unassigned devices, you can exit the tool or use it to make any changes to the configuration that you require.

**Related links**

Using the HPSSA tool on page 99

## Clearing the RAID arrays for non-recording servers using the HPSSA tool

### Before you begin

Ensure that:

- You have a keyboard, mouse, and monitor.
- You have backed up any important data.
- You have launched the HPSSA tool.
- You have installed the 4 x 300 GB hard drives for all core servers.

**Note:**

Do not remove hard disk drives while the tool is executing.

### About this task

Use this procedure to clear the four hard drives to one RAID 10 array on the HP ProLiant DL360 G9 non-recording core servers.

### Procedure

1. Check for any arrays and logical devices on the left panel: In the **Controller Devices** sub-menu, look at the text under the **Logical Devices** menu.

   If there are no arrays or logical devices, configure the RAID arrays using the HPSSA tool.
2. In the central panel, click the **Clear Configuration** button.
3. On the resulting message, double-click the **Clear** button.
4. Double-click the **Finish** button.

### Next steps

Configure the RAID arrays using the HPSSA tool.

**Related links**

Using the HPSSA tool on page 99

## Clearing the RAID arrays for recording servers using the HPSSA tool

### Before you begin

Ensure that:

- You have a keyboard, mouse, and monitor.
- You have backed up any important data.
- You have launched the HPSSA tool.
- You have installed the 4 x 300 GB hard drives for all core servers.
- You have installed the 4 x 900 GB hard drives from the Avaya Aura® Conferencing upgrade kit for recording servers.

✱ **Note:**

Do not remove hard disk drives while the tool is executing.

### About this task

Use this procedure to clear the eight hard drives to two RAID 10 arrays on the HP ProLiant DL360 G9 recording servers.

### Procedure

1. Check for any arrays and logical devices on the left panel: In the **Controller Devices** sub-menu, look at the text under the **Logical Devices** menu.

   If there are no arrays or logical devices, configure the RAID arrays using the HPSSA tool.

2. If you want to clear both RAID arrays, in the central panel, click the **Clear Operation** button.

   a. On the resulting message, double-click the **Clear** button.

   b. Double-click the **Finish** button.

3. If you want to clear the RAID array in bays 5–8, in the central panel, click the **Array B — 1 Logical Drive(s)** option.

   a. In the right panel, click **Delete Array**.

   b. On the resulting message, double-click the **Yes** button.

   c. Double-click the **Finish** button.

4. If you want to clear the RAID array in bays 1–4 in the central panel, click the **Array A — 1 Logical Drive(s)** option.
    a. In the right panel, click **Delete Array**.
    b. On the resulting message, double-click the **Yes** button.
    c. Double-click the **Finish** button.

### Next steps

Configure the RAID arrays using the HPSSA tool.

**Related links**

Using the HPSSA tool on page 99

## Clearing the RAID arrays for cascading servers using the HPSSA tool

### Before you begin

Ensure that:

- You have a keyboard, mouse, and monitor.
- You have backed up any important data.
- You have launched the HPSSA tool.
- You have installed the 2 x 300 GB hard drives for all cascading servers.

**Note:**

Do not remove hard disk drives while the tool is executing.

### About this task

Use this procedure to clear the two hard drives to one RAID 1 array on the HP ProLiant DL360 G9 cascading servers.

### Procedure

1. Check for any arrays and logical devices on the left panel: In the **Controller Devices** sub-menu, look at the text under the **Logical Devices** menu.

    If there are no arrays or logical devices, configure the RAID arrays using the HPSSA tool.
2. In the central panel, click the **Clear Configuration** button.
3. On the resulting message, double-click the **Clear** button.
4. Double-click the **Finish** button.

### Next steps

Configure the RAID arrays using the HPSSA tool.

**Related links**

Using the HPSSA tool on page 99

# Chapter 7: Installing software for Avaya Aura® and Turnkey deployments on baremetal servers

## Introduction to software installation

This chapter provides installation information for the following:

- Linux operating system and base level packages
- Linux patches
- Element Manager
- Avaya Aura® Media Server

Two DVDs of the software components (Platform and Application Bundle) are provided with the hardware.

**Related links**

Software installation procedure for SMB on page 110
Software installation procedure for medium enterprises on page 113
Software installation procedure for large enterprises on page 115
Software installation procedure for adding additional media servers on page 118

## Software installation procedure for SMB

The following table provides a high-level view of the tasks involved in installing the platform and applications software.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Ensure you have planned your deployment layout and populated your data in the Avaya Aura® Conferencing Intelligent Workbook. | See Before you begin checklist on page 81. | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 2 | Download HP documentation | See Downloading HP documentation on page 87 | | |
| 3 | Install hardware | See Installing the server in the rack on page 93 | The hardware requirements for Avaya Aura® Conferencing are the same whether you are installing the product in an Avaya Aura® deployment or a Turnkey deployment. In both cases, it is the HP ProLiant DL360 G9 server. | |
| 4 | Review the prerequisites. | See Prerequisites for software installation on page 119 | | |
| 5 | Configure RAID arrays. | See Managing Hewlett Packard Smart Arrays on page 97 | | |
| 6 | Install the Avaya Aura® Conferencing Platform on the primary Element Manager server | See Installing the AAC Platform on page 121 | | |
| 7 | If your deployment is a redundant deployment, install the Avaya Aura® Conferencing Platform on the secondary Element Manager server | See Installing the AAC Platform on page 121 | | |
| 8 | Install the components for Avaya Aura® Conferencing | Depending on your deployment type, see:<br>• Installing the components for Avaya Aura® Conferencing for Avaya Aura® on page 132<br>• Installing the components for Avaya Aura® Conferencing for Turnkey on page 141 | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 9 | Ensure that you install the latest patches. | See *Upgrading Avaya Aura® Conferencing*, which is available on https://support.avaya.com/. This guide describes all of the patching procedures. | There are two types of patches for Avaya Aura® Conferencing:<br>• Operating System patches<br>• Application bundle patches<br>Ensure that you have the latest of both types of patch. | |
| 10 | Access Element Manager Console using local login | See Accessing Element Manager Console using local login on page 158 | | |
| 11 | Install the Avaya Aura® Conferencing license key | Depending on your deployment type, see:<br>• Licensing for Avaya Aura® deployments on page 171<br>• Licensing for Turnkey deployments on page 163 | | |
| At this point, the installation is complete and the remaining tasks are configuration tasks. For the most part, the configuration of a Turnkey deployment is the same as a Avaya Aura® deployment. The notable exceptions are:<br>• For Turnkey deployments, you must configure the PBX as a SIP entity on Avaya Aura® Conferencing. See Configuration checklist on page 218.<br>• For Turnkey deployments, you must configure users using LDAP or Provisioning Manager. See Options for user provisioning on page 228.<br>This current document describes the Avaya Aura® Conferencing configuration tasks. In addition, the *Avaya Aura® Conferencing Port Matrix Guide*, which is available on https://support.avaya.com/ lists the ports which Avaya Aura® Conferencing uses.<br>Avaya recommends taking a backup of your Avaya Aura® Conferencing system after you install it. For the most part, the process of backing up a Turnkey deployment is the same as a Avaya Aura® deployment. The notable exception is:<br>• For Turnkey deployments, the License Manager is embedded and must be backed up. See Backing up WebLM on page 164.<br>For more information on the backup procedure, see *Migrating Avaya Aura® Conferencing*, which is available on https://support.avaya.com/ and *Upgrading Avaya Aura® Conferencing*, which is also available on https://support.avaya.com/. | | | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| Avaya also recommends increasing the security settings on your Avaya. For the most part, the process of increasing the security for a Turnkey deployment and a Avaya Aura® deployment is the same. For more information, see Hardening Avaya Aura® Conferencing on page 593. | | | | |

**Related links**

Introduction to software installation on page 110

## Software installation procedure for medium enterprises

The following table provides a high-level view of the tasks involved in installing the platform and applications software.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Ensure you have planned your deployment layout and populated your data in the Avaya Aura® Conferencing Intelligent Workbook. | See Before you begin checklist on page 81. | | |
| 2 | Download HP documentation | See Downloading HP documentation on page 87 | | |
| 3 | Install hardware | See Installing the server in the rack on page 93 | The hardware requirements for Avaya Aura® Conferencing are the same whether you are installing the product in an Avaya Aura® deployment or a Turnkey deployment. In both cases, it is the HP ProLiant DL360 G9 server. | |
| 4 | Review the prerequisites. | See Prerequisites for software installation on page 119 | | |
| 5 | Configure RAID arrays. | See Managing Hewlett Packard Smart Arrays on page 97 | | |
| 6 | Install the Avaya Aura® Conferencing Platform on the primary Element Manager server | See Installing the AAC Platform on page 121 | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 7 | If your deployment is a redundant deployment, install the Avaya Aura® Conferencing Platform on the secondary Element Manager server | See Installing the AAC Platform on page 121 | | |
| 8 | Install the components for Avaya Aura® Conferencing | Depending on your deployment type, see:<br>• Installing the components for Avaya Aura® Conferencing for Avaya Aura® on page 132<br>• Installing the components for Avaya Aura® Conferencing for Turnkey on page 141 | | |
| 9 | Ensure that you install the latest patches. | See *Upgrading Avaya Aura® Conferencing*, which is available on https://support.avaya.com/. This guide describes all of the patching procedures. | There are two types of patches for Avaya Aura® Conferencing:<br>• Operating System patches<br>• Application bundle patches<br>Ensure that you have the latest of both types of patch. | |
| 10 | Access Element Manager Console using local login | See Accessing Element Manager Console using local login on page 158 | | |
| 11 | Install the Avaya Aura® Conferencing license key | Depending on your deployment type, see:<br>• Licensing for Avaya Aura® deployments on page 171<br>• Licensing for Turnkey deployments on page 163 | | |

*Table continues…*

<table>
<tr><th>#</th><th>Task</th><th>Description</th><th>Notes</th><th>✔</th></tr>
<tr><td colspan="5">At this point, the installation is complete and the remaining tasks are configuration tasks. For the most part, the configuration of a Turnkey deployment is the same as a Avaya Aura® deployment. The notable exceptions are:<br>• For Turnkey deployments, you must configure the PBX as a SIP entity on Avaya Aura® Conferencing. See Configuration checklist on page 218.<br>• For Turnkey deployments, you must configure users using LDAP or Provisioning Manager. See Options for user provisioning on page 228.<br>This current document describes the Avaya Aura® Conferencing configuration tasks. In addition, the <i>Avaya Aura® Conferencing Port Matrix Guide</i>, which is available on https://support.avaya.com/ lists the ports which Avaya Aura® Conferencing uses.<br>Avaya recommends taking a backup of your Avaya Aura® Conferencing system after you install it. For the most part, the process of backing up a Turnkey deployment is the same as a Avaya Aura® deployment. The notable exception is:<br>• For Turnkey deployments, the License Manager is embedded and must be backed up. See Backing up WebLM on page 164.<br>For more information on the backup procedure, see <i>Migrating Avaya Aura® Conferencing</i>, which is available on https://support.avaya.com/ and <i>Upgrading Avaya Aura® Conferencing</i>, which is also available on https://support.avaya.com/.<br>Avaya also recommends increasing the security settings on your Avaya. For the most part, the process of increasing the security for a Turnkey deployment and a Avaya Aura® deployment is the same. For more information, see Hardening Avaya Aura® Conferencing on page 593.</td></tr>
</table>

**Related links**

Introduction to software installation on page 110

## Software installation procedure for large enterprises

The following table provides a high-level view of the tasks involved in installing the platform and applications software.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Ensure you have planned your deployment layout and populated your data in the Avaya Aura® Conferencing Intelligent Workbook. | See Before you begin checklist  on page 81. | | |
| 2 | Download HP documentation | See Downloading HP documentation on page 87 | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 3 | Install hardware | See Installing the server in the rack on page 93 | The hardware requirements for Avaya Aura® Conferencing are the same whether you are installing the product in an Avaya Aura® deployment or a Turnkey deployment. In both cases, it is the HP ProLiant DL360 G9 server. | |
| 4 | Review the prerequisites. | See Prerequisites for software installation on page 119 | | |
| 5 | Configure RAID arrays. | See Managing Hewlett Packard Smart Arrays on page 97 | | |
| 6 | Install the Avaya Aura® Conferencing Platform on the primary Element Manager server, primary Web Conferencing Server (WCS), and primary Avaya Aura® Media Server. | See Installing the AAC Platform on page 121 | | |
| 7 | If your deployment is a redundant deployment, install the Avaya Aura® Conferencing Platform on the secondary Element Manager server. Also, install the secondary Web Conferencing server and the secondary Avaya Aura® Media Servers. | See Installing the AAC Platform on page 121 | | |
| 8 | Install the components for Avaya Aura® Conferencing | Depending on your deployment type, see:<br>• Installing the components for Avaya Aura® Conferencing for Avaya Aura® on page 132<br>• Installing the components for Avaya | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| | | Aura® Conferencing for Turnkey on page 141 | | |
| 9 | Ensure that you install the latest patches. | See *Upgrading Avaya Aura® Conferencing*, which is available on https://support.avaya.com/. This guide describes all of the patching procedures. | There are two types of patches for Avaya Aura® Conferencing:<br>• Operating System patches<br>• Application bundle patches<br>Ensure that you have the latest of both types of patch. | |
| 10 | Access Element Manager Console using local login | See Accessing Element Manager Console using local login on page 158 | | |
| 11 | Install the Avaya Aura® Conferencing license key | Depending on your deployment type, see:<br>• Licensing for Avaya Aura® deployments on page 171<br>• Licensing for Turnkey deployments on page 163 | | |
| At this point, the installation is complete and the remaining tasks are configuration tasks. For the most part, the configuration of a Turnkey deployment is the same as a Avaya Aura® deployment. The notable exceptions are:<br>• For Turnkey deployments, you must configure the PBX as a SIP entity on Avaya Aura® Conferencing. See Configuration checklist on page 218.<br>• For Turnkey deployments, you must configure users using LDAP or Provisioning Manager. See Options for user provisioning on page 228.<br>This current document describes the Avaya Aura® Conferencing configuration tasks. In addition, the *Avaya Aura® Conferencing Port Matrix Guide*, which is available on https://support.avaya.com/ lists the ports which Avaya Aura® Conferencing uses.<br>Avaya recommends taking a backup of your Avaya Aura® Conferencing system after you install it. For the most part, the process of backing up a Turnkey deployment is the same as a Avaya Aura® deployment. The notable exception is:<br>• For Turnkey deployments, the License Manager is embedded and must be backed up. See Backing up WebLM on page 164.<br>For more information on the backup procedure, see *Migrating Avaya Aura® Conferencing*, which is available on https://support.avaya.com/ and *Upgrading Avaya Aura® Conferencing*, which is also available on https://support.avaya.com/. | | | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| Avaya also recommends increasing the security settings on your Avaya. For the most part, the process of increasing the security for a Turnkey deployment and a Avaya Aura® deployment is the same. For more information, see Hardening Avaya Aura® Conferencing on page 593. | | | | |

**Related links**

Introduction to software installation on page 110

## Software installation procedure for adding additional media servers

The following table provides a high-level view of the tasks involved in configuring and deploying additional media servers.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Download HP documentation | See Downloading HP documentation on page 87 | | |
| 2 | Install hardware | See Installing the server in the rack on page 93 | The hardware requirements for Avaya Aura® Conferencing are the same whether you are installing the product in an Avaya Aura® deployment or a Turnkey deployment. In both cases, it is the HP ProLiant DL360 G9 server. | |
| 3 | Review the prerequisites. | See Prerequisites for software installation on page 119 | | |
| 4 | Configure RAID arrays. | See Managing Hewlett Packard Smart Arrays on page 97 | | |
| 5 | Install the Avaya Aura® Conferencing Platform on the additional server | See Installing the AAC Platform on page 121 | | |
| 6 | Install the Avaya Aura® Media Server platform on the additional server. | See Installing Avaya Media Server  on page 153 | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 7 | Add additional Avaya Aura® Media Server host. | See Adding additional Avaya Media Server hosts on page 242 | | |
| 8 | Add an Avaya Aura® Media Server network element. | See Adding an Avaya Media Server network element on page 243 | | |
| 9 | Deploy an Avaya Aura® Media Server network element. | See Deploying a Network Element instance on page 244 | | |
| 10 | Create a new media server cluster.<br>**Note:**<br>Skip this step if you want to add an additional Avaya Aura® Media Server to an existing media server cluster. | See Creating a new cluster on page 245 | | |
| 11 | Add an additional Avaya Aura® Media Server to media server cluster. | See Adding an additional Avaya Media Server to an existing media server cluster on page 245 | | |

**Related links**

Introduction to software installation on page 110

## Prerequisites for software installation

- The deployment layout type has been chosen based on the capacity and scaling requirements.
- The data in the Avaya Aura® Conferencing Intelligent Workbook has been completed and the required number of IP addresses obtained.
- Obtain the latest installation disks for Linux and software installation:
  - Avaya Aura® Conferencing Platform DVD ROM
  - Application Bundle DVD-ROM
- The target servers meet the following requirements:
  - All Application Servers have the same hardware type with the same disk, CPU, memory, and network interface configuration according to the appropriate deployment layout.

  - All servers meet the minimum hardware and configuration requirements for Avaya Aura® Conferencing.
  - All servers are connected and installed into the target environment including cables and network connections.
  - All servers have the Motherboard BIOS and the disk controller BIOS settings configured to ensure installation of the server platform software.
- The host environment meets the following:
  - Networking is in place to host the target servers and it is configured to route traffic between servers, firewalls, routers, switches, DMZ, and any other equipment in the host network, for example, management stations.
  - Up to two NTP clock sources available for the system to receive clocking information.
  - Up to three DNS servers available for the system to resolve addresses
  - A desktop computer or server (other than the one hosting the target server), that can execute ICMP ping requests.
  - A Windows based PC with Internet Explorer 8.0 or 9.0, or Firefox 4.0 or later.
  - A desktop computer or server that is synchronized to the same external NTP clock sources used by the target servers.
- Obtain any certificates that are to be used from either an Enterprise Certificate Authority or from some other well-known trusted Certificate Authority.
- If you are installing Avaya Aura® Conferencing with Avaya Aura®:
  - The following components must be installed and operational prior to installing Avaya Aura® Conferencing.
    - Avaya Aura® Session Manager Release 6.2
    - Avaya Aura® System Manager Release 6.2 or 6.3
  - The following data has been gathered:
    - Avaya Aura® System Manager OAM IP address
    - Avaya Aura® Session Manager Signaling Service IP Address
- If you are installing Avaya Aura® Conferencing with another SIP-based PBX (Turnkey)
  - One of the following PBX/SIP Entities must be installed and operational prior to installing Avaya Aura® Conferencing:
    - Communication Manager Release 5.2.1 or 6.0.1
    - Avaya Communication Server 1000 Release 7.5
    - IP Office Release 9.0
  - Media Connection Preservation must be enabled for the SIP line between IP Office Release 9.0 and Avaya Aura® Conferencing Turnkey. If Media Connection Preservation is not enabled, the IP Office calls will be dropped in the event of a failover from an active application server to a standby application server.

# Installing the AAC Platform

This section provides the procedures for installing the Avaya Aura® Conferencing platform operating system and base level packages to the target servers required for the initial system installation.

## Before you begin

- Ensure that you have the skills required to install, configure, and upgrade Avaya Aura® Conferencing. For a list of the required core competencies, see Audience on page 26. Before undertaking any advanced procedures, you must complete the required Avaya Aura® Conferencing training, as listed in Training on page 23. Avaya recommends that you download all available Avaya Aura® Conferencing documentation, as listed in Documentation on page 20.
- Obtain the latest Avaya Aura® Conferencing Platform DVD-ROM and the Application Bundle DVD-ROM.
- Obtain the Linux service pack patch disk.
- Ensure that the DVD-ROM drive is selected as the first priority boot device in the system BIOS (typically configured during initial BIOS setup).
- Ensure that the server backup file is on a remote server
- Ensure access to the server console through a locally attached keyboard and monitor or a Keyboard, video card, and monitor (KVM) switch.
- Plan and identify the deployment layout including all network IP addresses, hostnames, and FQDNs using the Avaya Aura® Conferencing Intelligent Workbook.

  **Note:**

  Avaya recommends that you implement DNS lookup to synchronize domain names and IP addresses for the Avaya Aura® Conferencing solution. If your deployment does not support DNS lookup, see DNS and Avaya Aura Conferencing on page 671.
- Plan and identify any expansion servers using the Avaya Aura® Conferencing Intelligent Workbook.

## About this task

Avaya Aura® Conferencing must be installed on a Linux platform. Use the following procedure to install the Avaya Aura® Conferencing platform operating system and base level packages on the HP ProLiant DL360 G9 server.

## Procedure

1. Insert the AAC Platform DVD-ROM, and reboot the server.

   The following message on the installation welcome screen appears:

   ```
   Welcome to the MCP Core Linux System Installer
   ```
2. At the boot prompt, type `install-kvm`, and press **Enter**.
3. To check the integrity of the system, type `y`, and press **Enter**.

**Important:**

If you do not check the integrity, a defective DVD-ROM or optical drive can go undetected and result in an installation failure.

If you receive a message indicating that the integrity check has failed, follow the recommendations to clean or replace DVD-ROM, or replace the optical drive.

If there are no issues with the integrity check, the installation continues to the next prompt.

4. At the prompt, `Would you like to view licensing information? (Y/N) [Y]?`
   - Type `n` if you have already viewed the licensing information from a previous server installation, and press **Enter**. Proceed to Step 5 on page 122.

     **OR**
   - Type `y` to acknowledge the licensing attributes, and press **Enter**.

     You are prompted for the following:

     a. At the prompt, `Enter Selection`, select one of the following:
        - Enter `1` for a Licensing overview.
        - Enter `2` for a summary of Open Source RPMs and Licenses.
        - Enter `3` to exit.

     b. Press **Enter** until the `Enter Selection` prompt appears again.

     c. At the prompt to acknowledge the licensing information, type `y`, and press **Enter**.

**Warning:**

In the following step, the installer erases all existing data on the attached disk drives.

5. At the `Continue [c], abort [a]` prompt, type `c` to continue, and press **Enter**.
6. At the prompt, `Do you want to keep this date and time (Y/N) [Y].`
   - Type `y` to keep the current system date and time, and press **Enter**. Proceed to the next step.
   - Type `n` to change the system date and time from the BIOS clock, and press **Enter**. Proceed to Modifying the BIOS clock on page 123.
7. The installer attempts to identify the hardware type of the target server, perform one of the following:
   - If the installer has detected your target server as a known reference server:

     Type `A` to accept and proceed to Step 9 on page 123 or type `O` and proceed to Classifying the hardware environment on page 124.

     **OR**
   - The installer does not detect your target server as a known reference server:

     At the prompt, type a number that corresponds to your hardware type, and press **Enter**.

8. At the prompt, `Is this information correct? y/n`, type `y` to continue or `n` to correct.
9. At the prompt to choose the install type, type `1` to select Manual Install, and press **Enter**.
10. On the System Configuration screen, at the prompt, `Press the Enter Key to begin configuration`, press **Enter**, and proceed to Configuring the system on page 125.
11. Configure the NTP clock source settings. See Configuring the NTP clock on page 127.
12. Configure the Syslog server. See Configuring the Syslog Server on page 129.
13. Encrypt the data disk. See Encrypting the recording data disk on page 131.

### Next steps

Proceed to Installing the components for Avaya Aura® Conferencing for Avaya Aura® on page 132 or Installing the components for Avaya Aura® Conferencing for Turnkey on page 141.

**Related links**

Modifying the BIOS clock on page 123
Classifying the hardware environment on page 124
Configuring the system on page 125
Configuring the NTP clock on page 127
Configuring the Syslog Server on page 129
Encrypting the recording data disk on page 131

## Modifying the BIOS clock

During the software installation of the target server, you can modify the BIOS clock.

### Before you begin

The procedure for Installing the license attributes is completed.

### Procedure

1. At the prompt `Enter the month (1-12) [x]` type the number that represents the current month, and press **Enter**. For example, 1 represents January and 12 represents December.
2. At the prompt `Enter the day (1-xx) [x]` type the value for the current date, and press **Enter**.
3. At the prompt `Enter the year (YYYY) [xxxx]` type the current year, and press **Enter**.
4. At the prompt `Enter the hour (0-23) [xx]` type the value for the current hour using the 24–hour clock, and press **Enter**. For example, the first hour of the day is 0 and the last hour of the day is 23.

5. At the prompt `Enter the minutes (0-59) [xx]`, type the minutes using the 24–hour clock, and press **Enter**. For example, the first minute of the day is 0 and the last minute of the day is 59.
6. At the prompt `Do you want to keep this date and time (Y/N) [Y] ?`, type `y` to save your changes, and press **Enter**.

### Result

The BIOS clock is modified. To verify the procedure:

- Log in as the root user and check that date is set correctly by running `date` command.

### Next steps

Refer back to Step 7 on page 122 in Installing the AAC Platform on page 121 to continue with the installation process.

**Related links**

Installing the AAC Platform on page 121

## Classifying the hardware environment

During the software installation of the target server, you can classify the server hardware as either a known reference server or as a non-reference server. The installer usually determines this classification but it can be manually changed in the following procedure.

**Note:**

If two disks have been detected and the reference server does not support the RAID-1 software, the two physical disks are identified by the installer as a single disk drive. If a single disk has been detected and the reference server requires two disks for RAID-1 disk mirroring, the installation aborts.

### About this task

Configure the target server as a reference or non-reference server and to change the default hardware.

### Procedure

1. If the installer identifies the target server as a reference server, choose the number in the list that corresponds to the hardware type, and proceed to Step 3. For example, type `2` for HP ProLiant DL360 G9.
2. If the installer does not detect the server as a reference server, a list of hardware options appears, type `1` for Other, and press **Enter**. Proceed to Step 4.
3. If the target server is a reference server, at the prompt, `Hardware Environment: <hardware platform>`, for example, HP ProLiant DL360 G9, type `y`, and press **Enter**.
4. If the installer detects a non-reference server, at the prompt, `Hardware Environment: Other`, type `y`, and press **Enter**.

5. A message appears to indicate the size and number of disks. If the physical disk configuration matches the requirements for the reference server, press **Enter** to continue.

   The hardware is configured.

### Result

The hardware is classified. To verify the procedure:

1. Log in as the root user and run the command `swversion.pl | grep Hardware`.
2. Check that hardware type is the same as was entered during platform installation.

   For example, HP ProLiant DL360 G9.

### Next steps

Refer back to Step 9 on page 123 in Installing the AAC Platform on page 121 to continue with the installation process.

**Related links**

Installing the AAC Platform on page 121

## Configuring the system

During the Linux operating system installation, you are prompted to configure the usernames, passwords, server time, IP address, DNS, and hardware type for your system.

### About this task

Configure the system.

### Procedure

1. On the Network Configuration screen, at the prompt `Enter hostname (FQDN)`, type a hostname for the server.

   **Note:**

   You must enter the fully qualified domain name (FQDN) in the `Enter hostname` field, rather than the short name.

2. At the prompt `Enter bond name [bond0]`, press **Enter** to accept the default.

   A list of available Ethernet Network interfaces appears.

3. At the prompt `Enter the first slave [eth0]` type the Bond0 Slave0 value for the server or press **Enter** to accept the default value.
4. At the prompt `Enter the second slave [eth1]`, type the Bond0 Slave1 value for the server or press **Enter** to accept the default value.
5. At the prompt `Enter VLAN ID (0=no VLAN) (0-4094)`, type 0 as this is not supported, and press **Enter**.
6. At the prompt `Enter subnet name [sn0]`, press **Enter** to accept the default value.

7. At the prompt `Enter IP address`, type the Network IP address of the server, and press **Enter**.
8. At the prompt, `Enter subnet prefix length (1-32)`, type the Network Prefix of the server, and press **Enter**.
9. At the prompt `Enter gateway IP address`, type the Network Default Gateway, and press **Enter**.
10. At the prompt `Do you want to configure DNS Client? (Y/N) [Y]`, type `y` and press **Enter**.

    The following prompt appears:

    ```
    Please select one of the following actions:
    - [A]dd Domain Suffix(es)
    - Re[S]elect all Domain Suffix(es)
    - [C]ontinue
    ```
11. At the prompt, type `c` to continue or `a` to add suffixes, and press **Enter**.
12. At the prompt `How many DNS Servers would you like to reference (1-3) [1]`, type the number of available DNS servers, and press **Enter**.
13. At the prompt `Enter DNS Server`, type the IP address of the DNS server, and press **Enter**.
14. At the prompt `You entered "<IP address>". Is this correct? (Y/N) [N]`, verify the IP address.
15. If the IP address is correct, type `y` and press **Enter**.
16. The Timezone Selection screen appears. At the prompt `Enter Region (1-62)`, type the number that corresponds to the Timezone Field1 for the target server, and press **Enter**.
17. If you see the screen Timezone Selection for Region, at the prompt `Enter Timezone`, type the number that corresponds to the Timezone Field2 for the target server, and press **Enter**.
18. The Configuration Validation screen appears. Type `y` to accept the values or type `n` to reenter the information. Press **Enter**.

## Result

The system is configured. To verify the procedure:

1. Log in as the root user.
2. Check that the Hostname is set correctly by running `hostname` command.
3. Check that the network is configured correctly:

    Run `cat /admin/nwk/mcpNwkCfg.xml` and check that bond name, slave names, VLAN ID, subnet name, server IP, Network Prefix and Network Default Gateway are configured correctly.

    Run `ifconfig` and check that bond name, slave names, subnet name, server IP, and Network Default Gateway are configured correctly.

Run `ping <server IP>` to check that system is a ping-able from an external server.

4. Check that the DNS is configured correctly:

   Run `cat /etc/resolv.conf | grep name` and check that all configured DNS servers are present at displayed list.

   Run `cat /etc/resolv.conf | grep search` and check that all configured Domain Suffix are present at displayed list.

   Run ``nslookup `hostname` `` and check that the DNS hostname name was resolved successfully.

   Run `nslookup <server IP>` and check that the server IP was resolved successfully.

5. Check that the timezone is configured correctly.

   Run `tzConfig.pl`. Then, press **ENTER** and check that default value for Timezone is the same as it was entered during installation. Press **ENTER** in order to complete working with `tzConfig.pl`.

### Next steps

Refer back to Step 11 on page 123 in Installing the AAC Platform on page 121 to continue with the installation process.

#### Related links

Installing the AAC Platform on page 121

## Configuring the NTP clock

During the software installation, you are prompted to configure the Network Time Protocol (NTP) settings.

**Note:**

You must use the same NTP sources that are being used on the System Manager. For more information about the NTP server IP addresses, see the Avaya Aura® Conferencing Intelligent Workbook.

### About this task

Configure the NTP clock settings.

### Procedure

1. At the prompt, `Please indicate the Clock Source function of this server:`

   - `1. Primary Clock Source server (primary Element Manager server machine)`. For example, EMServer1.
   - `2. Secondary Clock Source server (secondary Element Manager server machine)`. For example, EMServer2. If you select this option, continue to Step 8 on page 128.

- `3. This server is NOT a Clock Source server (all other server machines)`. If you select this option, continue to Step 5 on page 128.

  `Select an option (1-3):`

  **Note:**

  If this is a non-redundant layout and you are configuring a server hosting Element Manager, type `1`, and press **Enter**.

2. The primary clock source server requires an external clock. At the prompt, `Select External Clock for time source(s) external to this server.`

   `Select Internal clock to use the system clock as the time source.`

   `E — External Clock Source (IP Addresses)`

   `I — Internal Clock (Unreliable)`

   `Select an option (E, I):` Type `e`, and press **Enter**.

3. At the prompt `How many external clock sources would you like to reference (1-2) [1]`, type a number based on the following:

   - If both External Clock Source #1 and External Clock Source #2 have an IP address, type `2`, and press **Enter**.
   - If there is only one external clock source, type `1` or press **Enter** to accept the default.

4. At the prompt `Enter Clock Source IP address #1`, type the IP address for the external clock source.

   If you have more than one clock source, a second prompt appears.

5. At the prompt, `Enter IP Address of Primary Clock Source`, type the IP address for the Primary Clock Source, and press **Enter**.

   If you have a secondary clock source, a second prompt appears.

6. At the prompt, `Enter IP Address of Secondary Clock Source`, type the IP address for the Secondary Clock Source, and press **Enter**.

   **Note:**

   For non-redundant layouts, you can use the same IP address for primary and secondary clock source.

7. At the prompt, `Is this information correct? Y/N [N]`, type `y` to continue or `n` to correct.

8. At the prompt, `Please indicate the Clock Source function of this server:`

   - 1 `Primary clock Source server (primary Element Manager server machine)`
   - 2 `Secondary Clock Source server (secondary Element Manager server machine)`

- 3 `This server is NOT a Clock Source server (all other server machines)`

`Select an option (1-3) [1]`. Type `2`, and press **Enter**.

9. At the prompt, `The Secondary Clock Source server requires the use of an external clock.`

   Select External Clock for time source(s) external to this server.

   Select Internal Clock to use the local system clock as the time source.

   `E - External Clock source (IP Addresses)`

   `I - Internal Clock (Unreliable)`

   `Select an option (E, I):` Type `e`, and press **Enter**.
10. At the prompt, `How many external clock sources would you like to reference (1-2) [1]`, type `2`, and press **Enter**.
11. At the prompt, `Enter IP Address of Primary Clock Source:`, type the IP address, and press **Enter**.

### Result

The NTP clock is configured. To verify the procedure:

1. Log in as the root user.
2. Run the command `ntpConfig.pl` and at the following prompt `Do you wish to configure/display the NTP configuration? Enter 'c' to configure, 'd' to display, or 'q' to quit [c/d/q]:`, enter `d` and check that NTP servers are configured correctly and time is synchronized with NTP server.
3. At the prompt `Do you wish to configure/display the NTP configuration? Enter 'c' to configure, 'd' to display, or 'q' to quit [c/d/q]:`, enter `q` to complete work with `ntpConfig.pl` script.
4. Run following commands and check that the NTP shift is small and there is no issues:

```
service ntpd stop

ntpdate <ntpServer_ip>

service ntpd start
```

### Next steps

Refer back to Step 12 on page 123 in Installing the AAC Platform on page 121 to continue with the installation process.

#### Related links

Installing the AAC Platform on page 121

## Configuring the Syslog Server

During the Linux operating system installation, you are prompted to configure the Syslog Server.

### About this task

Configure the settings for the Syslog Server, if required.

### Procedure

1. On the Syslog Configuration screen, at the prompt `Do you wish to configure a Syslog Server IP address (Y/N) [N]?`, type `n` (default), and press **Enter**. Proceed to the next section for viewing the user accounts and passwords.
   - If you want to configure the Syslog Server IP address, type `y`, and press **Enter**. Proceed to the next step.
2. At the prompt `Enter the Syslog Server IP address`, type the value for the Syslog IP address, and press **Enter**.

### Result

The syslog is configured. To verify the procedure:

1. Log in as the root user and run the command `syslogConfig.pl`.
2. At the `Do you wish to configure/unconfigure/display the SysLog Server IP Address? Enter 'c' to configure, 'u' to unconfigure, 'd' to display, or 'q' to quit [c/u/d/q]:` prompt, enter `d` in order to see if the syslog is configured correctly.
3. At the `Do you wish to configure/unconfigure/display the SysLog Server IP Address? Enter 'c' to configure, 'u' to unconfigure, 'd' to display, or 'q' to quit [c/u/d/q]:` prompt, enter `q` to complete working with the `syslogConfig.pl` script.
4. Run the command `ntpConfig.pl`.
5. At the `Do you wish to configure/display the NTP configuration? Enter 'c' to configure, 'd' to display, or 'q' to quit [c/d/q]:` prompt, enter `c` in order to emulate the ntp changing. This is required in order to send a message to the syslog.
6. Press **ENTER** and accept the default values.

   Wait until the `ntpConfig.pl` script completes.
7. Take a look in syslog logs on the syslog server and check that the logs about the ntp update appeared.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

#### Related links

Installing the AAC Platform on page 121

## Encrypting the recording data disk

During the Linux operating system installation, you are prompted to encrypt the data disk.

### About this task

The purpose of this task is to encrypt the recording data disk. This is an optional task. You can choose not to encrypt the recording data disk.

### Procedure

1. On the **Encrypt Recording Data Disk** screen, at the prompt **Do you wish to encrypt the recording data disk (Y/N) [N]?**
   - If you do not wish to encrypt the recording data disk, type `n` (default), and press **Enter**. Proceed to the next section for viewing user accounts and passwords.
   - If you wish to encrypt the recording data disk, type `y`, and press **Enter**. Proceed to the next step.
2. At the prompt **Enter the encryption secure phrase**, type the secure phrase for the encrypted data disk.

   ⚠ **Warning:**

   After the installation, you need to provide a platform back-up. If you do not back up the platform then during the platform failure, all information on the recording data disk is lost. There is no other way to restore or recreate the encrypted secure phrase.
3. On the **Configuration Validation** screen, if the values are correct, type `y`, and press **Enter** to accept and continue or type `n`, and press **Enter** to reenter the data.

### Result

The recording data disk is configured correctly. To verify the procedure:

1. Log in as the root user and run the command `cat /admin/userinfo.txt | grep DataDisk`.
   - For an encrypted system, `recDataDiskEncryption=1` should appear.
   - For a non-encrypted system, `recDataDiskEncryption=0` should appear.
2. Before running the following checks for systems with two disks, see Formatting and mounting the second RAID on page 151. Run the command `ls -l /dev/mapper | grep DataDisk`.
   - For an encrypted system, the following should appear:
     ```
     lrwxrwxrwx 1 root root      7 Jan 14 09:49 vg_data-lv_var_mcp_datadisk -> ../
     dm-2
     lrwxrwxrwx 1 root root      8 Jan 14 09:49 vg_data-lv_var_mcp_edatadisk -> ../
     dm-11
     ```
   - For a non-encrypted system, the following should appear:
     ```
     lrwxrwxrwx 1 root root      7 Jan 14 09:49 vg_data-lv_var_mcp_datadisk -> ../
     dm-2
     ```

3. Run the command `cat /proc/mounts | grep datadisk`.

    - For an encrypted system, the following should appear:

      ```
      /dev/mapper/vg_data-lv_var_mcp_edatadisk /var/mcp/data ext4
      rw,relatime,barrier=1,data=ordered 0 0
      ```

    - For a non-encrypted system, the following should appear:

      ```
      /dev/mapper/vg_data-lv_var_mcp_datadisk /var/mcp/data ext4
      rw,relatime,barrier=1,data=ordered 0 0
      ```

4. Run the command `ls -l /var/mcp | grep data`. The following should appear:

    ```
    drwxrwx--- 3 ntappsw ntappgrp      4096 Jan 19 15:39 data
    lrwxrwxrwx 1 ntappsw ntappgrp        13 Jan 19 15:43 datadisk -> /var/mcp/data
    ```

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

**Related links**

Installing the AAC Platform on page 121

## Installing the components for Avaya Aura® Conferencing for Avaya Aura®

Use the following procedure for a fresh installation of the Avaya Aura® Conferencing components on a new system. At this point, if you wish to use VMware to perform certain aspects of this procedure, consult Installing AAC for Avaya Aura® using VMware on page 173.

**Note:**

Currently, Avaya Aura® Conferencing does not support VMware for the SMB-sized solution. You can only using VMware for medium or large deployments.

### Before you begin

- Ensure that you have administrator access on all servers.
- Ensure that the AAC Platform operating system is installed.
- Ensure that the Application Bundle DVD-ROM content is in `/var/mcp/extract`.
- Obtain the installation properties and identified the tags file based on your deployment type. To assist, use the Avaya Aura® Conferencing Intelligent Workbook.
- Obtain the required number of IP addresses for your deployment layout type.
- Stop any network elements that are currently running.
- Ensure that there is no media server instance, of the same or a later version, already installed.
- Ensure that you have the skills required to install, configure, and upgrade Avaya Aura® Conferencing. For a list of the required core competencies, see Audience on page 26. Before

undertaking any advanced procedures, you must complete the required Avaya Aura® Conferencing training, as listed in Training on page 23. Avaya recommends that you download all available Avaya Aura® Conferencing documentation, as listed in Documentation on page 20.

## About this task

This procedure uses an automated mcpInstaller script that installs the following components in the following order:

- Avaya Aura® Conferencing Application Database: The Avaya Aura® Conferencing application requires a database in which all configuration, provisioning, and operational data is stored. The database software is installed on the server(s) that host the Element Manager.
- Avaya Aura® Conferencing Application software: This is the core conferencing application. After the installation is complete, the primary instance (0) of Element Manager is running, along with the primary and optionally (if redundant system) secondary database instances. The Element Manager administration console can be accessed after this step is complete.
- Avaya Aura® Media Server: The Avaya Aura® Conferencing application requires one or more Avaya Aura® Media Servers for media processing. The mcpInstaller script can install the media server automatically in all (SMB, medium, and large) configurations. If you are implementing a redundant deployment, the mcpInstaller automatically installs a primary and a secondary Avaya Aura® Media Server.
- Install certificates signed by the Avaya Aura® System Manager Certificate Authority: The Avaya Aura® Conferencing application requires certificates signed by the Avaya Aura® System Manager Certificate Authority. They are used by Network Element instances.

**Note:**

You cannot use the mcpinstaller installation tool to install media servers in remote locations. This is due to the potential network delays that could be encountered during the installation process. To install remote media servers individually, see Installing Avaya Media Server on page 153. Remote locations, in this context, are locations that are separated from the core application servers.

## Procedure

1. Log on to EMServer1 as ntappadm through ssh or directly at the server console.
2. At the password prompt, type the password for ntappadm.

   When you first log on to the system, you may be prompted to change your password.
3. Type `mcpInstaller`, and press **Enter**.
4. Type the password for ntappadm, and press **Enter**.
5. Type `y` to continue with the installation.

   The following prompt appears:

   ```
   Searching for installation software...

   The following application load instances have been found:

   [1] /var/mcp/extract/dvd_AAC_MCP_18.X.X.XX_XXXX-XX-XX-
   XXXX_coreApps.iso
   ```

```
[2] Optical Drive

Please select which load instance you wish to install [1..2]:
```

6. Type the number of the Application Bundle you want to use, and press **Enter**.
7. At the prompt, type `y` to continue with the installation.
8. At the prompt, type `y` to continue with the installation.
9. Ensure that no network elements are currently running and that there is no media server of the same or a later version already installed.
10. Type `y` to continue with the installation.

    The following prompt appears:

    ```
    Select the deployment type for AAC

    [1] AAC with Avaya Aura

    [2] AAC connected to a SIP based PBX (CM, CS1k, IPO, etc)

    Please enter number [1 to 2] of selection:
    ```

11. Type `1` to install AAC with Avaya Aura®or type `2` to install AAC connected to a SIP based PBX.
12. Press **Enter**.
13. Type `n` to continue with the installation.

    The following prompt appears:

    ```
    Please select the Staging File that will be used

    [1] Staging_AAC_Large_Redundant

    [2] Staging_AAC_Large_Simplex

    [3] Staging_AAC_Medium_Redundant

    [4] Staging_AAC_Medium_Simplex

    [5] Staging_AAC_SMB_Redundant

    [6] Staging_AAC_SMB_Simplex

    Please enter number [1 to 6] of selection:
    ```

14. Type the number of the staging file that you want to use and press **Enter**.

    The following prompt appears:

    ```
    Looking for loads in /var/mcp/loads/

    Only one load found: MCP_18.X.X.XX_XXXX-XX-XX-XXXX

    Use this load?(Y/N)[Y]:
    ```

15. Type `y` to continue with the installation.

The following prompt appears:

```
Please select configuration to use
[1] AAC_Large_Dell610-24GB12Core
[2] AAC_Large_HPDL360G7-12GB12Core
[3] AAC_Large_HPDL360G7-12GB8Core
[4] AAC_Large_HPDL360G7-36GB12Core
[5] AAC_Large_HPDL360G8-16GB6Core
[6] AAC_Large_HPDL360G8-32GB12Core
[7] AAC_Large_HPDL360G9-32GB6Core
[8] AAC_Large_HPDL360G9-32GB16Core
[9] AAC_Large_S8800-24GB8Core
[10] AAC_Medium_Dell610-24GB12Core
[11] AAC_Medium_HPDL360G7-36GB12Core
[12] AAC_Medium_HPDL360G8-16GB6Core
[13] AAC_Medium_HPDL360G8-32GB12Core
[14] AAC_Medium_HPDL360G9-32GB6Core
[15] AAC_Medium_HPDL360G9-32GB16Core
[16] AAC_Medium_S8800-24GB8Core
[17] AAC_SMB_Dell610-24GB12Core
[18] AAC_SMB_HPDL360G7-36GB12Core
[19] AAC_SMB_HPDL360G8-16GB6Core
[20] AAC_SMB_HPDL360G8-32GB12Core
[21] AAC_SMB_HPDL360G9-32GB6Core
[22] AAC_SMB_HPDL360G9-32GB16Core
[23] AAC_SMB_Other-8GB4Core
[24] AAC_SMB_S8800-24GB8Core
Please enter number [1 to 24] of selection:
```

16. Type the number of the configuration you want to use, and press **Enter**.
17. Type `n` to continue with the installation.
18. At the prompt `Please enter the value for <tag name> [<default>]`, provide the information from the Avaya Aura® Conferencing Intelligent Workbook, and press **Enter**.

    The list of tags for the various deployment layout types is shown in Populating tags on page 136.
19. A summary of the installation parameters appears. Type `y` to accept and begin the installation or `n` to edit the information before installing, or `Q` to quit the installer.

    **Note:**

    This process can take more than 30 minutes to complete.
20. At the prompts `Please enter the Enrollment Password` and `Please reenter the Enrollment Password` type and confirm the enrollment password.

    **Note:**

    If you have chosen AAC connected to a SIP-based PBX this step does not appear.
21. **(Optional)** If you are installing the secondary system in a redundant deployment with automatic disaster recovery (ADR), the following prompt is displayed:

    ```
    Please enter the EM User password:
    ```

    At this prompt, enter the same password as the Element Manager administrator password in the primary system.

22. At the **Does the Thumbprint above match the Thumbprint of the Avaya Aura System Manager Certificate Authority** prompt, verify the thumbprint and enter **Y**.

### Result

The components are installed. To verify the installation:

1. Run the `swversion.pl` script. Check the `Database Version` and `AAC Applications Load Information` sections to verify that the expected database version and MCP load was installed..
2. Run the `/var/mcp/run/MCP_18.X/EM_0/bin/getInstanceState.pl` script.

   You should see an **ACTIVE** message.
3. Check that you can login to the Element Manager Console. For more information, see Accessing Element Manager Console using local login on page 158.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

### Related links

Populating tags on page 136

## Populating tags

The following tables identify the parameters that are required to configure your specific deployment layout. Tags are used to enter configuration data such as IP address and hostname for all elements of a particular deployment layout. You are prompted to enter these tags after starting the mcpInstaller script on the initial install. The tags can also be manually modified by using the command **`populateTagsFile.pl -t <tag file name>`**. Prior to starting your installation, populate the tags in the Configuration Data tab of the Avaya Aura® Conferencing Intelligent Workbook. The following tables contain the tag file names by deployment layout type.

**Note:**

To use single sign-on (SSO), the System Manager FQDN, Element Manager FQDN, and Provisioning Client FQDN (if required) must belong to the same root domain.

### SMB Simplex and Medium Simplex

**Table 10: Tag population—SMB Simplex & Medium Simplex**

| Installation properties and tag prompts | Property or tag name | Example value |
|---|---|---|
| Service IPv4 address of Element Manager | TAG_EM_INT_OAM_SVC_ADDR | 192.168.209.1 |

*Table continues…*

| Installation properties and tag prompts | Property or tag name | Example value |
|---|---|---|
| Service IPv4 address of Accounting Manager | TAG_AM1_INT_OAM_SVC_ADDR | 192.168.209.2 |
| Service IPv4 address of Application Server | TAG_AS1_INT_OAM_SVC_ADDR | 192.168.209.3 |
| Media IPv4 address of the primary Avaya Aura® Media Server | TAG_EM_SVR1_MEDIA_ADDR | 192.168.209.4 |
| Service IPv4 address of the primary Web Conferencing Server | TAG_WCS1_SVC_ADDR | 192.168.209.5 |
| FQDN for the Service IPv4 address of the Element Manager | TAG_EM_SVC_FQDN | emsrv.domain.com |
| FQDN for the Provisioning Manager | TAG_PROV1_SVC_FQDN | prov1.domain.com |
| FQDN for the Collaboration Agent Manager | TAG_CA1_SVC_FQDN | ca1.domain.com |
| FQDN for the Document Conversion Server | TAG_DCS1_SVC_FQDN | dcs1.domain.com |
| FQDN for the Web Conferencing Server | TAG_WCS1_SVC_FQDN | wcs1.domain.com |
| Site Name of the Avaya Aura® Conferencing installation. | TAG_SITE_NAME | UpdateMeSite |
| Site Long Name of the Avaya Aura® Conferencing installation. | TAG_SITE_LONG_NAME | UpdateMeSiteLongName |

## SMB Redundant & Medium Redundant

**Table 11: Tag population—SMB Redundant & Medium Redundant**

| Installation properties and tag prompts | Property or tag name | Value |
|---|---|---|
| Internal OAM (Default) IPv4 address of the secondary Element Manager server | TAG_EM_SVR2_INT_OAM_ADDR | 192.168.209.1 |
| Service IPv4 address of Element Manager | TAG_EM_INT_OAM_SVC_ADDR | 192.168.209.2 |
| Service IPv4 address of Accounting Manager | TAG_AM1_INT_OAM_SVC_ADDR | 192.168.209.3 |
| Service IPv4 address of Application Server | TAG_AS1_INT_OAM_SVC_ADDR | 192.168.209.4 |

*Table continues…*

| Installation properties and tag prompts | Property or tag name | Value |
|---|---|---|
| Media IPv4 address of the primary Avaya Aura® Media Server | TAG_EM_SVR1_MEDIA_ADDR | 192.168.209.5 |
| Media IPv4 address of the secondary Avaya Aura® Media Server | TAG_EM_SVR2_MEDIA_ADDR | 192.168.209.6 |
| Service IPv4 address of the primary Web Conferencing Server | TAG_WCS1_SVC_ADDR | 192.168.209.7 |
| Service IPv4 address of the secondary Web Conferencing Server | TAG_WCS2_SVC_ADDR | 192.168.209.8 |
| FQDN for the Service IPv4 address of the Element Manager | TAG_EM_SVC_FQDN | emsvc.domain.com |
| FQDN for the primary Provisioning Manager | TAG_PROV1_SVC_FQDN | prov1.domain.com |
| FQDN for the secondary Provisioning Manager | TAG_PROV2_SVC_FQDN | prov2.domain.com |
| FQDN for the primary Web Conferencing Server | TAG_WCS1_SVC_FQDN | wcs1.domain.com |
| FQDN for the secondary Web Conferencing Server | TAG_WCS2_SVC_FQDN | wcs2.domain.com |
| FQDN for the primary Collaboration Agent Manager | TAG_CA1_SVC_FQDN | ca1.domain.com |
| FQDN for the secondary Collaboration Agent Manager | TAG_CA2_SVC_FQDN | ca2.domain.com |
| FQDN for the primary Document Conversion Server | TAG_DCS1_SVC_FQDN | dcs1.domain.com |
| FQDN for the secondary Document Conversion Server | TAG_DCS2_SVC_FQDN | dcs2.domain.com |
| Site Name of the Avaya Aura® Conferencing installation. | TAG_SITE_NAME | UpdateMeSite |
| Site Long Name of the Avaya Aura® Conferencing installation. | TAG_SITE_LONG_NAME | UpdateMeSiteLongName |

## Large Simplex

**Table 12: Tag population—Large Simplex**

| Installation properties and tag prompts | Property or tag name | Value |
|---|---|---|
| Service IPv4 address of Element Manager | TAG_EM_INT_OAM_SVC_ADDR | 192.168.209.1 |

*Table continues…*

| Installation properties and tag prompts | Property or tag name | Value |
|---|---|---|
| Service IPv4 address of Accounting Manager | TAG_AM1_INT_OAM_SVC_ADDR | 192.168.209.2 |
| Service IPv4 address of Application Server | TAG_AS1_INT_OAM_SVC_ADDR | 192.168.209.3 |
| IPv4 address of the primary Media and Web Conferencing Server | TAG_MWC_SVR1_ADDR | 192.168.209.4 |
| Service IPv4 address of the primary Web Conferencing Server | TAG_WCS1_SVC_ADDR | 192.168.209.5 |
| Media IPv4 address of the primary Avaya Media Server | TAG_MWC_SVR1_MEDIA_ADDR | 192.168.209.6 |
| Service IPv4 address of the primary Document Conversion Server | TAG_DCS1_SVR_ADDR | 192.168.209.7 |
| FQDN for the Service IPv4 address of the Element Manager | TAG_EM_SVC_FQDN | emsvc.domain.com |
| FQDN for the primary Provisioning Manager | TAG_PROV1_SVC_FQDN | prov1.domain.com |
| FQDN for the primary Collaboration Agent Manager | TAG_CA1_SVC_FQDN | ca1.domain.com |
| FQDN for the primary Web Conferencing server | TAG_WCS1_SVC_FQDN | wcs1.domain.com |
| FQDN for the primary Document Conversion Server | TAG_DCS1_SVC_FQDN | dcs1.domain.com |
| Site Name of this AAC installation | TAG_SITE_NAME | UpdateMeSite |
| Site Long Name of this AAC installation | TAG_SITE_LONG_NAME | UpdateMeSiteLongName |

## Large Redundant

**Table 13: Tag population—Large Redundant**

| Installation properties and tag prompts | Property or tag name | Example value |
|---|---|---|
| Internal OAM (Default) IPv4 address of the secondaryElement Manager server | TAG_EM_SVR2_INT_OAM_ADDR | 192.168.209.1 |
| Service IPv4 address of Element Manager | TAG_EM_INT_OAM_SVC_ADDR | 192.168.209.2 |
| Service IPv4 address of Accounting Manager | TAG_AM1_INT_OAM_SVC_ADDR | 192.168.209.3 |

*Table continues…*

| Installation properties and tag prompts | Property or tag name | Example value |
|---|---|---|
| Service IPv4 address of Application Server | TAG_AS1_INT_OAM_SVC_ADDR | 192.168.209.4 |
| IPv4 address of the primary Media and Web Conferencing Server | TAG_MWC_SVR1_ADDR | 192.168.209.5 |
| Service IPv4 address of the primary Web Conferencing Server | TAG_WCS1_SVC_ADDR | 192.168.209.6 |
| IPv4 address of the secondary Media and Web Conferencing Server | TAG_MWC_SVR2_ADDR | 192.168.209.7 |
| Service IPv4 address of the secondary Web Conferencing Server | TAG_WCS2_SVC_ADDR | 192.168.209.8 |
| Media IPv4 address of the primary Avaya Media Server | TAG_MWC_SVR1_MEDIA_ADDR | 192.168.209.9 |
| Media IPv4 address of the secondary Avaya Media Server | TAG_MWC_SVR2_MEDIA_ADDR | 192.168.209.10 |
| Service IPv4 address of the primary Document Conversion Server | TAG_DCS1_SVR_ADDR | 192.168.209.11 |
| Service IPv4 address of the secondary Document Conversion Server | TAG_DCS2_SVR_ADDR | 192.168.209.12 |
| FQDN for the Service IPv4 address of the Element Manager | TAG_EM_SVC_FQDN | emsvc.domain.com |
| FQDN for the primary Provisioning Manager | TAG_PROV1_SVC_FQDN | prov1.domain.com |
| FQDN for the secondary Provisioning Manager | TAG_PROV2_SVC_FQDN | prov2.domain.com |
| FQDN for the primary Collaboration Agent Manager | TAG_CA1_SVC_FQDN | ca1.domain.com |
| FQDN for the secondary Collaboration Agent Manager | TAG_CA2_SVC_FQDN | ca2.domain.com |
| FQDN for the primary Web Conferencing server | TAG_WCS1_SVC_FQDN | wcs1.domain.com |
| FQDN for the secondary Web Conferencing server | TAG_WCS2_SVC_FQDN | wcs2.domain.com |

*Table continues…*

| Installation properties and tag prompts | Property or tag name | Example value |
|---|---|---|
| FQDN for the primary Document Conversion Server | TAG_DCS1_SVC_FQDN | dcs1.domain.com |
| FQDN for the secondary Document Conversion Server | TAG_DCS2_SVC_FQDN | dcs2.domain.com |
| Site Name of this AAC installation | TAG_SITE_NAME | UpdateMeSite |
| Site Long Name of this AAC installation | TAG_SITE_LONG_NAME | UpdateMeSiteLongName |

### Avaya Aura® System Manager and Session Manager

**Table 14: Tag population—Avaya Aura® System Manager and Session Manager**

| Installation properties and tag prompts | Property or tag name | Example value |
|---|---|---|
| IPv4 address of the System Manager | TAG_SMGR1_SVR_ADDR | 192.168.100.1 |
| IPv4 address of the Session Manager | TAG_ASM1_SVR_ADDR | 192.168.100.2 |
| FQDN for the Aura System Manager | TAG_SMGR1_FQDN | smgr.domain.com |
| SMGR SNMP Trap Listener Port (for Alarm forwarding) | TAG_SMGR_SNMP_TRAP_PORT | 162 |
| SMGR SNMP Community String (for Alarm forwarding) | TAG_SMGR_COMMUNITY_STRING | |

**Note:**

In a redundant system, with automatic disaster recovery (ADR), the System Manager and Session Manager addresses should be the same.

**Related links**

Installing the components for Avaya Aura Conferencing for Avaya Aura on page 132

## Installing the components for Avaya Aura® Conferencing for Turnkey

Use the following procedure for a fresh installation of the Avaya Aura® Conferencing components on a new system. At this point, if you wish to use VMware to perform certain aspects of this procedure, consult Installing AAC for Turnkey using VMware on page 198. In an Avaya Aura® Conferencing for Turnkey deployment, the conferencing software does use the Avaya Aura® solution stack. Instead, it uses an alternative PBX. In this context, the “Avaya Aura® solution stack” refers to staging and management software such as System Platform and System Manager. An alternative PBX might refer to Avaya Communication Server 1000 or Avaya IP Office.

**Note:**

Currently, Avaya Aura® Conferencing does not support VMware for the SMB-sized solution. You can only using VMware for medium or large deployments.

### Before you begin

- The AAC Platform operating system is installed with Domain Name Server (DNS) and Network Time Protocol (NTP) configured.
- You have downloaded the latest software application bundle.
- You have obtained the required number of IP addresses for your deployment layout type. Enter the information in the following table:

| Name | IP Address | Fully Qualified Domain Name (FQDN) |
|---|---|---|
| Primary Element Manager Server | | |
| Element Manager Service | | |
| Accounting Manager Service | | |
| Application Server Service | | |
| Media Server Media Address | | |
| Web Conferencing Server (WCS) Service | | |
| DNS Server | | |
| NTP Server | | |

- Stop any network elements that are currently running.
- Ensure that there is no media server instance, of the same or a later version, already installed.
- Ensure that you have administrator access on all servers.
- Ensure that you have the skills required to install, configure, and upgrade Avaya Aura® Conferencing. For a list of the required core competencies, see Audience on page 26. Before undertaking any advanced procedures, you must complete the required Avaya Aura® Conferencing training, as listed in Training on page 23. Avaya recommends that you download all available Avaya Aura® Conferencing documentation, as listed in Documentation on page 20.

### About this task

As an alternative to installing the application bundle from the DVD-ROM, you can install the application bundle using an ISO image file. Prior to running the `mcpInstaller` script, you can download an ISO image file from the Avaya Product Licensing and Delivery System (PLDS) and transfer this file to the `/var/mcp/extract/` directory on the Element Manager (EMServer1). The script prompts you to select whether you wish to install from the ISO image file or from the optical drive.

**Note:**

You cannot use the mcpinstaller installation tool to install media servers in remote locations. This is due to the potential network delays that could be encountered during the installation process. To install remote media servers individually, see Installing Avaya Media Server on page 153. Remote locations, in this context, are locations that are separated from the core application servers.

## Procedure

1. Log on to EMServer1 as ntappadm through ssh or directly at the server console.
2. At the prompt, change the directory by typing `cd var/mcp/install`.
3. Type `mcpInstaller`, and press **Enter**.
4. Type the password for ntappadm, and press **Enter**.

   When you first log on to the system, you may be prompted to change your password.
5. Type `y` to continue with the installation.

   The following prompt appears:

   ```
   Searching for installation software...

   The following application load instances have been found:

   [1] /var/mcp/extract/dvd_AAC_MCP_18.X.X.XX_XXXX-XX-XX-
   XXXX_coreApps.iso

   [2] Optical Drive

   Please select which load instance you wish to install [1..2]:
   ```
6. Type the number of the Application Bundle you want to use, and press **Enter**.
7. At the prompt, type `y` to continue with the installation.
8. At the prompt, type `y` to continue with the installation.
9. Ensure that no network elements are currently running and that there is no media server of the same or a later version already installed.
10. Type `y` to continue with the installation.

    The following prompt appears:

    ```
    Select the deployment type for AAC

    [1] AAC with Avaya Aura

    [2] AAC connected to a SIP based PBX (CM, CS1k, IPO, etc)

    Please enter number [1 to 2] of selection:
    ```
11. Type `2` to install Avaya Aura® Conferencing for Turnkey.
12. Press **Enter**.
13. Type `n` to continue with the installation.

The following prompt appears:

```
Please select the Staging File that will be used
[1] Staging_AAC_Large_Redundant
[2] Staging_AAC_Large_Simplex
[3] Staging_AAC_Medium_Redundant
[4] Staging_AAC_Medium_Simplex
[5] Staging_AAC_SMB_Redundant
[6] Staging_AAC_SMB_Simplex
Please enter number [1 to 6] of selection:
```

14. Type the number of the staging file that you want to use and press **Enter**.

    The following prompt appears:

    ```
    Looking for loads in /var/mcp/loads/
    Only one load found: MCP_18.X.X.XX_XXXX-XX-XX-XXXX
    Use this load?(Y/N)[Y]:
    ```

15. Type `y` to continue with the installation.

    The following prompt appears:

    ```
    Please select configuration to use
    [1] AAC_Large_Dell610-24GB12Core
    [2] AAC_Large_HPDL360G7-12GB12Core
    [3] AAC_Large_HPDL360G7-12GB8Core
    [4] AAC_Large_HPDL360G7-36GB12Core
    [5] AAC_Large_HPDL360G8-16GB6Core
    [6] AAC_Large_HPDL360G8-32GB12Core
    [7] AAC_Large_HPDL360G9-32GB6Core
    [8] AAC_Large_HPDL360G9-32GB16Core
    [9] AAC_Large_S8800-24GB8Core
    [10] AAC_Medium_Dell610-24GB12Core
    [11] AAC_Medium_HPDL360G7-36GB12Core
    [12] AAC_Medium_HPDL360G8-16GB6Core
    [13] AAC_Medium_HPDL360G8-32GB12Core
    [14] AAC_Medium_HPDL360G9-32GB6Core
    [15] AAC_Medium_HPDL360G9-32GB16Core
    [16] AAC_Medium_S8800-24GB8Core
    [17] AAC_SMB_Dell610-24GB12Core
    [18] AAC_SMB_HPDL360G7-36GB12Core
    [19] AAC_SMB_HPDL360G8-16GB6Core
    [20] AAC_SMB_HPDL360G8-32GB12Core
    [21] AAC_SMB_HPDL360G9-32GB6Core
    [22] AAC_SMB_HPDL360G9-32GB16Core
    [23] AAC_SMB_Other-8GB4Core
    [24] AAC_SMB_S8800-24GB8Core
    Please enter number [1 to 24] of selection:
    ```

16. Type the number of the configuration you want to use, and press **Enter**.
17. Type `n` to continue with the installation.

18. At the prompt `Please enter the value for <tag name> [<default>]`, provide the information from the Avaya Aura® Conferencing Intelligent Workbook, and press **Enter**.

    The list of tags for the various deployment layout types is shown in Populating tags on page 136.

19. A summary of the installation parameters appears. Type `y` to accept and begin the installation or `n` to edit the information before installing, or `Q` to quit the installer.

    **Note:**

    This process can take more than 30 minutes to complete.

20. **(Optional)** If you are installing the secondary system in a redundant deployment with automatic disaster recovery (ADR), the following prompt is displayed:

    ```
    Please enter the EM User password:
    ```

    At this prompt, enter the same password as the Element Manager administrator password in the primary system.

## Result

The components are installed. To verify the installation:

1. Run the `swversion.pl` script. Check the `Database Version` and `AAC Applications Load Information` sections to verify that the expected database version and MCP load was installed..
2. Run the `/var/mcp/run/MCP_18.X/EM_0/bin/getInstanceState.pl` script.

   You should see an **ACTIVE** message.
3. Check that you can login to the Element Manager Console. For more information, see Accessing Element Manager Console using local login on page 158.

## Next steps

Using the output link, launch the Element Manager Console and start each of the network elements (Accounting Manager, Application Server, Provisioning Manager, Web Conferencing Server (WCS), Web Conferencing Management Server (WCMS), Avaya Media Server, and so on). For more information, see Starting a network element instance on page 669.

Proceed to the Avaya Aura® Conferencing for Turnkey configuration steps. For more information, see Configuration checklist on page 218.

# Installing the media servers and recording media servers

## Recording and memory

### Introduction

In Avaya Aura® Conferencing, there are two possible scenarios in relation to recording and memory space capacity:

- If you order Avaya Aura® Conferencing with recording, the servers come with extra disks for recording. In this scenario, you must complete a specific set of tasks in order to install and configure the extra disks. For more information, see Checklist for a system with recording on page 146.
- If you order the recording feature at a later point in time, there is a disk kit to cover this purchase. In this scenario, you must complete a different set of tasks in order to install and configure the extra disks. At this point, you have two options:
  - You can add a new server for recording. For more information, see Checklist for adding a new server on page 147.
  - You can change the existing Avaya Aura® Media Server to make it a recording Avaya Aura® Media Server. For more information, see Checklist for repurposing your existing server on page 147.

**Note:**

These tasks apply equally to Avaya Aura® and Turnkey solutions.

### Checklist

**Table 15: If you order a system with recording**

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Ensure that you have configured RAID settings. | Using the Hewlett Packard™ Smart Storage Administrator (HPSSA) Tool on page 97 | | |
| 2 | Install the Avaya Aura® Conferencing platform. | Installing Avaya Aura Conferencing on page 121 | | |
| 3 | Format and mount the second RAID 10 | Formatting and mounting the second RAID 10 on page 151 | | |
| 4 | Install the Avaya Aura® Media Server. | Installing Avaya Media Server on page 153 | | |
| 5 | Configure recording. | Introduction to configuring the recording feature on page 339 | | |

**Table 16: If you order recording at a later date, as a disk kit and install a new server**

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Install 4 x 900 Gb hard drives into the HP DL360 G9 server | Installing the new 4 x 900 Gb drives on page 148 | | |
| 2 | Ensure that you have configured RAID settings. | Using the Hewlett Packard™ Smart Storage Administrator (HPSSA) Tool on page 97 | | |
| 3 | Extend the system to a two disk configuration. | Extending the system to a two disk configuration on page 149 | | |
| 4 | Format and mount the second RAID 10. | Formatting and mounting the second RAID 10 on page 151 | | |
| 5 | Install the Avaya Aura® Media Server. | Installing Avaya Media Server  on page 153 | | |
| 6 | Configure recording. | Introduction to configuring the recording feature on page 339 | | |

**Table 17: If you order recording at a later date, as a disk kit and repurpose your Avaya Aura® Media Server**

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Order the disk kit. | Contact your Avaya representative for more information about ordering. | | |
| 2 | Back-up your existing Avaya Aura® Media Server. | Backing up the Avaya media servers on page 155 | | |
| 3 | Stop and undeploy the Avaya Aura® Media Server network elements. | Stopping a network element instance on page 659<br>Undeploying a network element instance on page 659 | | |
| 4 | Uninstall Avaya Aura® Media Server. | | | |
| 5 | Install 4 x 900 Gb hard drives into the HP DL360 G9 server. | Installing the new 4 x 900 Gb drives on page 148 | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 6 | Ensure that you have configured RAID settings. | Using the Hewlett Packard™ Smart Storage Administrator (HPSSA) Tool on page 97 | | |
| 7 | Format the disk. | Formatting and mounting the second RAID 10 on page 151 | | |
| 8 | Install Avaya Aura® Media Server. | Installing the Avaya media server to the recording media server on page 154 | | |
| 9 | Deploy and start Avaya Aura® Media Server network elements. | Deploying a Network Element instance on page 244<br>Starting a network element instance on page 669 | | |

**Related links**

Disk kit on page 48

## Installing the 4 x 900 Gb hard drives into the HP ProLiant DL360 G9 server

### Before you begin

- You have backed up your Avaya Aura® Conferencing system.
- You have the memory upgrade kit, which contains the 4 x 900 Gb hard drives.
- You have the HP ProLiant DL360 G9 document set.

  For more information, see Downloading HP documentation G9 on page 87 and HP DL360 G9 document set on page 87.

### About this task

Use this procedure to install the 4 x 900 Gb hard drives from the Avaya Aura® Conferencing upgrade kit into the HP ProLiant DL360 G9 server.

### Procedure

1. Observe safety warnings.
2. Observe all ESD safety precautions before unwrapping the new hard drives.
3. Power off the Avaya Aura® Conferencing server.
4. Lift the release lever on hard drive bay 5 on the server and insert a new 900 Gb drive into hard drive bay 5.

For more information about the locations of the hard drive bays, see Front view of HP DL360 G9 Server on page 88.

5. When the locking tab engages on the 900 Gb hard drive, close the release lever to securely seat the 900 Gb hard drive in hard drive bay 5.
6. Repeat these steps for bays 6, 7, and 8.

## Extending the system to a two disk configuration

### Before you begin

Ensure:

- You have installed the 4 x 900 Gb hard drives the Avaya Aura® Conferencing upgrade kit.
- You have mounted the drives into bays 5-8 of the server and configured them as second RAID array.

### About this task

Use this task to extend the system to a two disk configuration model.

**Note:**

The recording feature requires the second logical drive. You must extend system to a two disk configuration model before installing the Avaya Aura® Media Server (AMS) platform.

### Procedure

1. Log on to the server as a user with the SSA role (for example, ntsysadm) through ssh or directly on the server console.
2. Enter `su –` to log on as root.
3. At the prompt password, type the root password, and press **Enter**.
4. Type `mcpDataDiskMgt.pl -q`, and press **Enter** to check that the second logical drive is available.

   The system should display information indicating that the RAID status is okay and the query command succeeded.

   An example of the output is:

   ```
   The expected data partition '/dev/sdb1' is not present on the system.
   The raid controller reports:
   A logical drive is available.
   It is 1.6 TB large and RAID 1+0.
   It has a RAID status of OK.
   Query command succeeded.
   ```
5. Type `mcpDataDiskMgt.pl -f`, and press **Enter** to format the second logical drive.

   The system displays the following information:

   ```
   Are you certain that you wish to reformat this disk? All information that is
   currently on it will be lost! (Y/N) [N]?
   ```

6. Type `y`, and press **Enter**.

   The system should display the following information:

   ```
   Format command succeeded.
   ```

7. Type `mcpDataDiskMgt.pl -q,` and press **Enter** to check that the second logical drive is ready for mounting.

   The system should display information indicating that the RAID status is okay and the query command succeeded.

   An example of the output is:

   For a non-encrypted system:

   ```
   The correct data partition is mounted on the expected mount point.
   The mount point information reported by the operating system is:
   /dev/mapper/vg_data-lv_var_mcp_datadisk /var/mcp/data ext4
   rw,nosuid,nodev,relatime,barrier=1,stripe=128,data=ordered 0 0
   The raid controller reports:
   A logical drive is available.
   It is 1.6 TB large and RAID 1+0.
   It has a RAID status of OK.
   Query command succeeded.
   ```

   For an encrypted system:

   ```
   The correct data partition is mounted on the expected mount point.
   The mount point information reported by the operating system is:
   /dev/mapper/vg_data-lv_var_mcp_edatadisk /var/mcp/data ext4
   rw,nosuid,nodev,relatime,barrier=1,stripe=128,data=ordered 0 0
   The raid controller reports:
   A logical drive is available.
   It is 1.6 TB large and RAID 1+0.
   It has a RAID status of OK.
   Query command succeeded.
   ```

8. Type `mcpDataDiskMgt.pl -u`, and press **Enter** to unmount the vg_data-lv_var_mcp_datadisk volume partition (If you have an encrypted system: vg_data-lv_var_mcp_edatadisk).

   The system should display the following information:

   ```
   Successfully un-mounted
   Umount command succeeded.
   ```

9. Type mcpDataDiskMgt.pl -q, and press **Enter** to extend system till 2 disks configuration.

   The system should display information indicating that the correct data partition is mounted.

   An example of the output for a non-encrypted system:

   ```
   The correct data partition is mounted on the expected mount point.
   The mount point information reported by the operating system is:
   /dev/mapper/vg_data-lv_var_mcp_datadisk /var/mcp/data ext4
   rw,nosuid,nodev,relatime,barrier=1,stripe=128,data=ordered 0 0
   The raid controller reports:
   A logical drive is available.
   It is 1.6 TB large and RAID 1+0.
   It has a RAID status of OK.
   Query command succeeded.
   ```

An example of the output for an encrypted system:

```
The correct data partition is mounted on the expected mount point.
The mount point information reported by the operating system is:
/dev/mapper/vg_data-lv_var_mcp_edatadisk /var/mcp/data ext4
rw,nosuid,nodev,relatime,barrier=1,stripe=128,data=ordered 0 0
The raid controller reports:
A logical drive is available.
It is 1.6 TB large and RAID 1+0.
It has a RAID status of OK.
Query command succeeded.
```

10. Type `mcpDataDiskMgt.pl -c`, and press **Enter** to unmount the vg_data-lv_var_mcp_datadisk volume partition. (If you have an encrypted system: vg_data-lv_var_mcp_edatadisk).

    The system displays the following information:

    ```
    Are you certain that you wish to move data from /dev/sda3 to /dev/sdb1?
    All information that is currently on it may be lost!
    (Y/N) [N]?
    ```

11. Type `y`, and press **Enter** . Please note that this operation may take a long time – do not interrupt it.

    The system should display the following information:

    ```
    Carry-over-data command succeeded.
    ```

# Formatting and mounting the second RAID

## Before you begin

- You have installed the 4 x 900 Gb hard drives from the Avaya Aura® Conferencing upgrade kit.
- You have mounted the drives into bays 5-8 of the server and configured them as second RAID array.

## About this task

Use this procedure to format and mount the second logical drive on the HP ProLiant DL360 G9 server.

**Note:**

The recording feature requires the second logical drive. You must format and mount the second logical drive before installing the Avaya Aura® Media Server (MS) platform.

## Procedure

1. Log on to the server as a user with the SSA role (for example, `ntsysadm`) through ssh or directly on the server console.
2. Enter **`su -`** to log on as root.
3. At the prompt `password`, type the root password, and press **Enter**.

4. Type `mcpDataDiskMgt.pl -q`, and press **Enter** to check that the second logical drive is available.

   The system should display information indicating that the RAID status is okay and the query command succeeded. An example of the output is:

   ```
   The expected data partition '/dev/sdb1' is not present on the system.
   The raid controller reports:
   A logical drive is available.
   It is 1.6 TB large and RAID 1+0..
   It has a RAID status of OK.
   Query command succeeded.
   ```

5. Type `mcpDataDiskMgt.pl -f`, and press **Enter** to format the second logical drive.

   The system displays the following information:

   ```
   Are you certain that you wish to reformat this disk?
   All information that is currently on it will be lost! (Y/N) [N]?
   ```

6. Type `y`, and press **Enter** .

   The system should display the following information:

   ```
   Format command succeeded.
   ```

7. Type `mcpDataDiskMgt.pl -q`, and press **Enter** to check that the second logical drive is ready for mounting.

   The system should display information indicating that the RAID status is okay and the query command succeeded. An example of the output is:

   For a non-encrypted system:

   ```
   The data disk logical volume partition /dev/mapper/vg_data-lv_var_mcp_datadisk is
   not currently mounted on /var/mcp/data.
   The raid controller reports:
   A logical drive is available.
   It is 1.6 TB large and RAID 1+0..
   It has a RAID status of OK.
   Query command succeeded.
   ```

   For an encrypted system:

   ```
   The data disk logical volume partition /dev/mapper/vg_data-lv_var_mcp_edatadisk is
   not currently mounted on /var/mcp/data.
   The raid controller reports:
   A logical drive is available.
   It is 1.6 TB large and RAID 1+0..
   It has a RAID status of OK.
   Query command succeeded.
   ```

8. Type `mcpDataDiskMgt.pl -m`, and press **Enter** to mount the second logical drive.

   The system should display the following information:

   ```
   Created mount point
   Mount command succeeded.
   ```

9. Type `mcpDataDiskMgt.pl -q`, and press **Enter** to check that the second logical drive is mounted.

The system should display information indicating that the correct data partition is mounted. An example of the output is:

For a non-encrypted system:

```
The correct data partition is mounted on the expected mount point.
The mount point information reported by the operating system is:
/dev/mapper/vg_data-lv_var_mcp_datadisk /var/mcp/data ext4
rw,nosuid,nodev,relatime,barrier=1,stripe=128,data=ordered 0 0
The raid controller reports:
A logical drive is available.
It is 1.6 TB large and RAID 1+0.
It has a RAID status of OK.
Query command succeeded.
```

For an encrypted system:

```
The correct data partition is mounted on the expected mount point.
The mount point information reported by the operating system is:
/dev/mapper/vg_data-lv_var_mcp_edatadisk /var/mcp/data ext4
rw,nosuid,nodev,relatime,barrier=1,stripe=128,data=ordered 0 0
The raid controller reports:
A logical drive is available.
It is 1.6 TB large and RAID 1+0.
It has a RAID status of OK.
Query command succeeded.
```

# Installing Avaya Aura® Media Server

## About this task

Use this procedure to install Avaya Aura® Media Server.

## Procedure

1. Log on to the server which hosts Avaya Aura® Media Server as a user with the SSA role (for example, `ntsysadm`) through SSH or directly at the server console.
2. At the prompt, type su – and press **Enter**.
3. Type the root password, and then press **Enter** to become the root user.
4. If this server is the primary Element Manager server then go to step 8.

   This procedure is for all types of servers. But if this is the primary Element Manager server, skip steps 5-7.

5. At the prompt, type `scp ntappadm@<IP address of the primary Element Manager server>:/var/mcp/loads/MCP_MediaServer_18*zip /var/mcp/loads/` and press **Enter**.
6. At the `Are you sure you want to continue connecting (yes/no)?` prompt, type `yes` and press **Enter**.
7. At the `ntappadm@<IP address>`'s password prompt, type the `ntappadm` password for the primary Element Manager server and press **Enter**.
8. At the prompt, type `mcpMsInstall.pl` press **Enter**.

The install script finds the zipped file. The system will detect more than one zipped file.

9. At the `Use this load? (Y/N) [Y]` prompt, type `y`, and press **Enter**
10. At the `Continue installation? (Y/N)` prompt, type `y` and press **Enter**.

### Result

The `Installation completed SUCCESSFULLY` message is displayed. The Avaya Aura® Media Server load is now installed.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

## Installing the Avaya Aura® Media Server to the recording media server

### About this task

Use this procedure to install the Avaya Aura® Media Server software to the recording media server.

### Procedure

1. Log on to the server which hosts Avaya Aura® Media Server as a user with the SSA role (for example, `ntsysadm`) through SSH or directly at the server console.
2. At the prompt, type `su -` and press **Enter**.
3. Type the root password, and then press **Enter** to become the root user.
4. At the prompt, type `mcpDataDiskMgt.pl -m` and press **Enter**.

   The data disk mounts.
5. If this server is the primary Element Manager server then go to step 9.
6. At the prompt, type `scp ntappadm@<IP address of the primary Element Manager server>:/var/mcp/loads/MCP_MediaServer_18*zip /var/mcp/loads/` and press **Enter**.
7. At the `Are you sure you want to continue connecting (yes/no)?` prompt, type `yes` and press **Enter**.
8. At the `ntappadm@<IP address of the primary Element Manager server>`'s password prompt, type the `ntappadm` password for the primary Element Manager server and press **Enter**.
9. At the prompt, type `mcpMsInstall.pl -dontStart` and press **Enter**.

   The install script finds the zipped file. The system will detect more than one zipped file.

10. At the `Use this load? (Y/N) [Y]` prompt, type `y`, and press **Enter**
11. At the `Continue installation? (Y/N)` prompt, type `y` and press **Enter**.
12. At the prompt, type `cd /var/mcp/ma/MAS/platdata/EAM/Backups/latest/` and press **Enter**.
13. At the prompt, type `tar -xf <AMS backup>` and press **Enter**.
14. At the prompt, type `exec bash` and press **Enter**.
15. At the prompt, type `amsupgrade /var/mcp/ma/MAS/platdata/EAM/Backups/latest/service_config.zip` and press **Enter**.
16. At the prompt, type `Y` to confirm that all services will be stopped.
17. Configure the SSH keys for conference recordings backup.

    See *Upgrading Avaya Aura® Conferencing*, which is available from the Avaya Support website: http://www.avaya.com/support.

### Result

The Avaya Aura® Media Server is installed.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

## Backing up the Avaya Aura® Media Server (MS)

### About this task

Use this procedure to backup the Avaya Aura® Media Server (MS).

### Procedure

1. Log on to the server which hosts Avaya Aura® Media Server (MS) as a user with the SSA role (for example, `ntsysadm`) through SSH or directly at the server console.
2. At the prompt, type `su` and press **Enter**.
3. Type the root password and press **Enter** to become the root user.
4. At the prompt type `msBackup.pl` and press **Enter**.

### Result

A backup summary report is displayed. The backup file is stored in the `/var/mcp/ma/MAS/platdata/EAM/Backups/latest` folder.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

**Related links**

Scheduling automatic backups on an Avaya Media Server on page 156

## Scheduling automatic backups on an Avaya Media Server

### Before you begin

- You are a user with the SSA role (for example, ntbackup and ntsysadm).
- You have root account privileges to access the backup files and log files.

### About this task

Use this procedure to schedule automatic backups for anAvaya Aura® Media Server .

**Important:**

Avaya recommends that you schedule backups for off-peak hours. The default backup time is 3:30 a.m.

### Procedure

1. Log on to the server as ntbackup or ntsysadm through SSH or an account with the SSA role.
2. Enter `sudo msScheduleBackup.pl`.
3. Enter the password (if required).
4. Enter `E` to schedule a daily backup.
5. Enter the time at which you want to perform the backup (hh:mm format).
6. Enter `Y` to confirm.
7. Enter `Q` to quit.

### Result

The backup is scheduled to occur at the specified time and will be stored in the /var/mcp/ma/MAS/platdata/EAM/Backups/latest folder. The backup file name will be in the format AUTO_msBackup_on_YYYY-MM-DD.tar.

A summary report of your activity is stored at /var/log/mas/msScheduleBackup.log.yyyymmdd_hhmmss. You can view the backup log file when you are logged on to the server with root privileges.

The backup file from the previous scheduled automatic backup will be moved to the /var/mcp/ma/MAS/platdata/EAM/Backups/AUTO_history folder. If the /var/mcp/ma/MAS/platdata/EAM/Backups/latest folder contains a manual backup file, the manual backup file is moved to the /var/mcp/ma/MAS/platdata/EAM/Backups folder.

**Note:**

The /var/mcp/ma/MAS/platdata/EAM/Backups/AUTO_history folder can contain up to two scheduled backup files (that is, the two latest scheduled backup files).

**Related links**

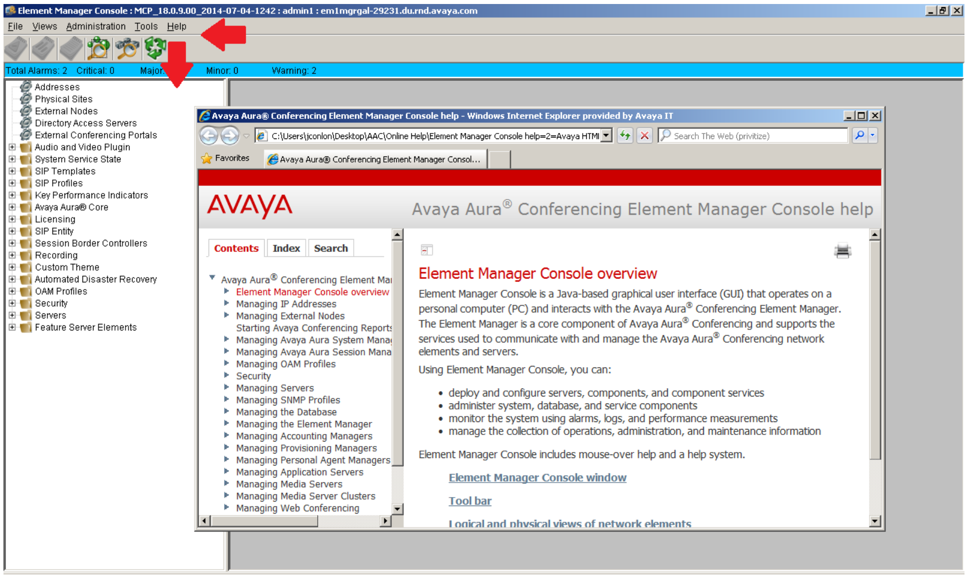
[Backing up the Avaya Aura Media Server (MS)](#) on page 155

## Deploying online help

Avaya Aura® Conferencing contains a number of online help files and online manuals to guide you through the process of installing, configuring, and maintaining your conferencing system. These online help files include:

- Online help for Element Manager
- Online help for the Provisioning Client
- Online help for Reports
- Online help for users of Collaboration Agent

By default, each of these online help packages is fully integrated with the component which it describes. So, for example, if you view help on Element Manager, you can access the Element Manager online help. The Element Manager online help file describes each of the Element Manager fields and describes many of the common procedures that you can perform using the Element Manager interface.


Element Manager Console : MCP_18.0.9.00_2014-07-04-1242 : admin1 : em1mgrgal-29231.du.rnd.avaya.com
File Views Administration Tools Help
Total Alarms: 2 Critical: 0 Major: Minor: 0 Warning: 2
Addresses
Physical Sites
External Nodes
Directory Access Servers
External Conferencing Portals
Audio and Video Plugin
System Service State
SIP Templates
SIP Profiles
Key Performance Indicators
Avaya Aura® Core
Licensing
SIP Entity
Session Border Controllers
Recording
Custom Theme
Automated Disaster Recovery
OAM Profiles
Security
Servers
Feature Server Elements
Avaya Aura® Conferencing Element Manager Console help - Windows Internet Explorer provided by Avaya IT
C:\Users\jconlon\Desktop\AAC\Online Help\Element Manager Console help=2=Avaya HTMl
Search The Web (privitize)
Favorites
Avaya Aura® Conferencing Element Manager Consol...
AVAYA
Avaya Aura® Conferencing Element Manager Console help
Contents
Index
Search
Avaya Aura® Conferencing Element Mai
Element Manager Console overview
Managing IP Addresses
Managing External Nodes
Starting Avaya Conferencing Reports
Managing Avaya Aura System Mana
Managing Avaya Aura Session Mana
Managing OAM Profiles
Security
Managing Servers
Managing SNMP Profiles
Managing the Database
Managing the Element Manager
Managing Accounting Managers
Managing Provisioning Managers
Managing Personal Agent Managers
Managing Application Servers
Managing Media Servers
Managing Media Server Clusters
Managing Web Conferencing

Element Manager Console overview

Element Manager Console is a Java-based graphical user interface (GUI) that operates on a personal computer (PC) and interacts with the Avaya Aura® Conferencing Element Manager. The Element Manager is a core component of Avaya Aura® Conferencing and supports the services used to communicate with and manage the Avaya Aura® Conferencing network elements and servers.

Using Element Manager Console, you can:

- deploy and configure servers, components, and component services
- administer system, database, and service components
- monitor the system using alarms, logs, and performance measurements
- manage the collection of operations, administration, and maintenance information

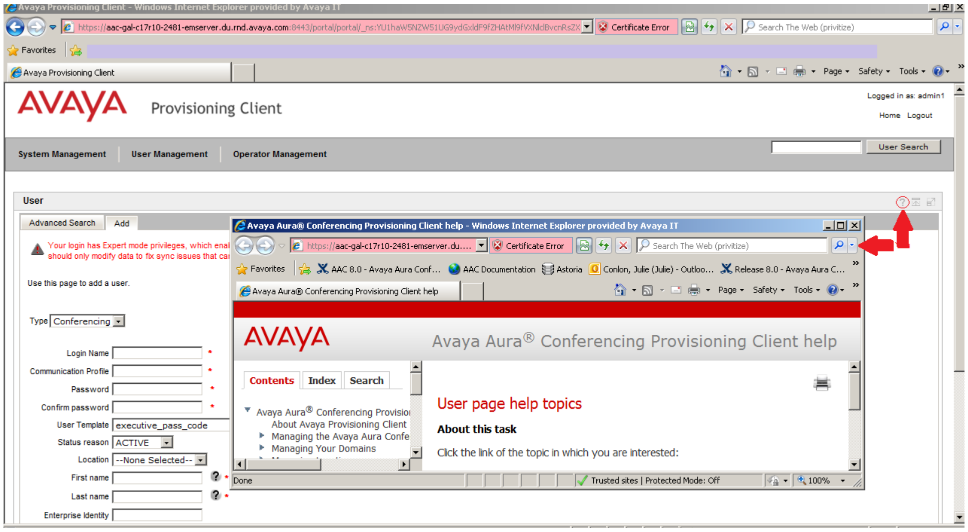
Element Manager Console includes mouse-over help and a help system.

Element Manager Console window

Tool bar

Logical and physical views of network elements

**Figure 17: Online Help for Element Manager**


Avaya Provisioning Client - Windows Internet Explorer provided by Avaya IT
https://aac-gal-c17r10-2481-emserver.du.rnd.avaya.com:8443/portal/portal/_ns:YU1haW5NZW51UG9ydGxldF9fZHAtMl9fVXNldBvcnRsZx
Certificate Error
Search The Web (privitize)
Favorites
Avaya Provisioning Client
Page
Safety
Tools
AVAYA
Provisioning Client
Logged in as: admin1
Home
Logout
System Management
User Management
Operator Management
User Search
User
Advanced Search
Add
Avaya Aura® Conferencing Provisioning Client help - Windows Internet Explorer provided by Avaya IT
https://aac-gal-c17r10-2481-emserver.du....
AAC 8.0 - Avaya Aura Conf...
AAC Documentation
Astoria
Conlon, Julie (Julie) - Outloo...
Release 8.0 - Avaya Aura C...
Avaya Aura® Conferencing Provisioning Client help
Contents
Index
Search
Done
Trusted sites | Protected Mode: Off
100%

Your login has Expert mode privileges, which enal
should only modify data to fix sync issues that ca

Use this page to add a user.

Type Conferencing

Login Name *

Communication Profile *

Password *

Confirm password *

User Template executive_pass_code

Status reason ACTIVE

Location --None Selected--

First name *

Last name *

Enterprise Identity

Avaya Aura® Conferencing Provisioning Client help

Avaya Aura® Conferencing Provisio
About Avaya Provisioning Client
Managing the Avaya Aura Confe
Managing Your Domains

User page help topics

About this task

Click the link of the topic in which you are interested:

**Figure 18: Online Help for the Provisioning Client**

In the case of the online help for users of Collaboration Agent, Avaya has translated the online help into several languages. The list of available languages conforms with the i18n and L10n (internationalization and localization standards). When users install the Collaboration Agent application, it chooses which language to display based on the computer's locale.

The online help files are packaged within the Avaya Aura® Conferencing software application bundle.

# Accessing Element Manager Console using local login

There are two ways to log on to the Element Manager (EM) Console:

- locally (as described in this procedure)
- single sign-on access through Avaya Aura® System Manager

**Note:**

To configure single sign-on, see Introduction to single-sign on for Element Manager Console and Provisioning Client on page 304.

## About this task

Use this procedure to log on to the Element Manager Console for the first time.

## Procedure

1. On the management PC, open the browser.
2. In the Address box, enter the following address: `https://<FQDN>:12121`.

   where *<FQDN>* is the EM Internal OAM Service Fully Qualified Domain Name (FQDN). This is the FQDN of the EM Internal OAM Service IP address.

3. Press **Enter**.

   A Web page appears displaying the IP address you entered and the link **Launch Element Manager Console**.

4. On the <IP address> page, click **Launch Element Manager Console**.

   ✱ **Note:**

   If Online Certificate Status Protocol (OSCP)-checking is not configured in your deployment, it can take up to 40 seconds to launch the Element Manager Console. If OSCP is not configured, contact your network administrator to configure it. If you do not intend to configure OSCP-checking in your deployment, you must switch off certificate revocation check in the Java settings on the management computer. To switch off certificate revocation check in Java settings:

   a. Navigate to Java Settings using the Windows Control Panel.

   b. Click the **Advanced** tab.

   c. Change **Perform certificate revocation checks on** to **Do not check**.

   d. Click **Apply**.

5. From the IPv4 Service Address box on the Element Manager Console window, select the IP address of the server running Element Manager Console.

6. Click **Connect**.

7. In the Element Manager Authentication window, click the **Accept the certificate for this session only** option button.

8. Click **Apply**.

   A connection is established to the active Element Manager instance.

9. In the UserID box on the Element Manager Console window, enter `admin`.

10. In the Current Password box, enter `admin`.

11. Click **Ok**.

    The Element Manager Console window appears. It is normal to see one major alarm displayed. (An orange alarm appears below the tool bar and displays `Major: 1`.) This alarm appears because the secondary instance (EM_1) of the Element Manager network element is not deployed or running. (The `Peer presumed failed` alarm is generated against the Element Manager network element.)

    ✱ **Note:**

    If you have a SMB Simplex, Medium Simplex or Large Simplex deployment, this alarm does not appear.

# Chapter 8: Installing the Avaya Aura® Conferencing (AAC) license key

## How licensing works

Licensing functionality operates in a different way, depending on your type of Avaya Aura® Conferencing deployment.

You can deploy Avaya Aura® Conferencing with the Avaya Aura® platform. The Avaya Aura® platform consists of Avaya Aura® System Manager, Avaya Aura® Session Manager, and Avaya Aura® System Platform. This type of deployment is called an Avaya Aura® deployment. Alternatively, you can deploy Avaya Aura® Conferencing without the Avaya Aura® platform. This type of deployment is called a Turnkey deployment.

In an Avaya Aura® deployment, licensing is supported on the Application Server and the Media Server. The License key is installed on the Web License Manager (WebLM) server which is co-resident with System Manager. The license key must be obtained prior to starting the deployment.

WebLM is a client/server model where numerous clients can share the same WebLM server and the same license key. For more information, see Installing the license key on on page 171.

In a Turnkey deployment, licensing is also supported by WebLM. However, in a Turnkey deployment, the WebLM server is embedded with Avaya Aura® Conferencing. For more information, see Applying a license key on page 164.

For both solutions, a grace period of 30 days exists for upgrades and new installations. Additionally, new upgrades and installations include a number of default licenses. If the licensing limits are exceeded, Avaya Aura® Conferencing displays full explanatory error messages to users. Licenses must be periodically renewed. If they are not renewed, they expire.

The license monitors:

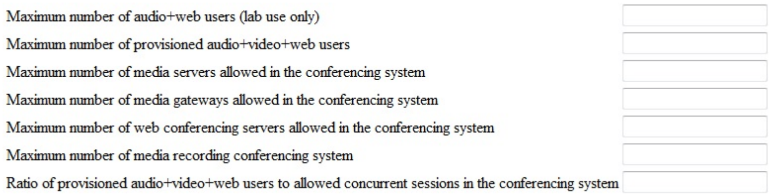
- Maximum number of provisioned audio, video, and web users
- Maximum number of media servers allowed in the Avaya Aura® Conferencing system
- Maximum number of recording Avaya Aura® Conferencing systems

**Related links**

License details on page 161

# License details

The Avaya Aura® Conferencing license has the following fields:



Maximum number of audio+web users (lab use only)

Maximum number of provisioned audio+video+web users

Maximum number of media servers allowed in the conferencing system

Maximum number of media gateways allowed in the conferencing system

Maximum number of web conferencing servers allowed in the conferencing system

Maximum number of media recording conferencing system

Ratio of provisioned audio+video+web users to allowed concurrent sessions in the conferencing system

**Figure 19: Avaya Aura® Conferencing license**

**Table 18: Feature names mapped to display names**

| Feature Name | Feature display name in the license | Description |
|---|---|---|
| VALUE_CONF_AUDIO_WEB_USERS | Maximum number of audio+web users (lab use only) | Not used. |
| VALUE_CONF_AUDIO_WEB_VIDEO_USERS | Maximum number of provisioned audio+video+web users | Maximum number of provisioned users supported on audio, video, and web.<br>If number of acquired licenses for users is not sufficient then an alarm is raised on Element Manager. An administrator can still add users (with or without video). The license does not impose restrictions on the numbers of users that the administrator can add.<br>**Note:**<br>A license is considered “consumed” once a user logs into Collaboration Agent. |
| VALUE_CONF_MEDIA_SERVERS | Maximum number of media servers allowed in the conferencing system | Maximum number of media servers allowed in the conferencing system |
| VALUE_CONF_MGW_SERVERS | Maximum number of media gateways allowed in the conferencing system | Not used. |
| VALUE_CONF_WEB_SERVERS | Maximum number of web conferencing servers allowed in the conferencing system | Not used. |

*Table continues…*

| Feature Name | Feature display name in the license | Description |
|---|---|---|
| VALUE_CONF_MEDIA_RECORDING_SYSTEMS | Maximum number of media recording conferencing system | Maximum number of conferencing systems that support media recording feature.<br>If Element Manger cannot acquire a license for recording, then the feature will be available during the 30 days grace period. After that time period, recording will be blocked for users. |
| VALUE_CONF_SESSION_RATIO | Ratio of provisioned audio+video +web users to allowed concurrent sessions in the conferencing system | Ratio of licensed users to allowed concurrent sessions.<br>To calculate ratio use the formula:<br>Ratio = (licensed audio/video/web users)/(allowed concurrent sessions)<br>This number should be between 1 and 100 – typically 10 for most customers.<br>So, for example, if you have VALUE_CONF_AUDIO_WEB_VIDEO_USERS = 100 and VALUE_CONF_SESSION_RATIO = 10, only 10 users can make a call at the same time |

Avaya Aura® Conferencing generates three derived session license values, based on the values of the VALUE_CONF_AUDIO_WEB_VIDEO_USERS and VALUE_CONF_SESSION_RATIO fields from the license key.

The application server will be able to handle up VALUE_CONF_AUDIO_WEB_VIDEO_USERS / VALUE_CONF_SESSION_RATIO sessions of each type (audio, video, and Web).

Once this value is reached, Avaya Aura® Conferencing denies any new sessions.

When the number of sessions of a particular type is close to the number of session licenses of a particular type, Avaya Aura® Conferencing raises an alarm on the application server. You can configure the threshold of this alarm. The default values: A minor alarm is raised at 70%, a major alarm is raised at 80%, and a critical alarm is raised at 90% usage.

If Avaya Aura® Conferencing cannot obtain any license information, the grace period starts for 30 days. In this time period, Avaya Aura® Conferencing will continue to operate, based on the last correct licensing values. There is no enforcement of a grace period if there was never any previous license. As soon as the grace period elapses, Avaya Aura® Conferencing rejects any new sessions. Avaya Aura® Conferencing raises a major alarm when the grace period begins (grace period alarm) and a critical alarm when the grace period ends (restricted mode alarm).

**Table 19: How the license is consumed for the various use cases**

| Starting conditions | Alternate scenarios | Consume |
|---|---|---|
| Audio only | | audio |
| | Add web[4] | + web |
| | Add video | + video |
| Web only[4] | | web |
| | Add audio | + audio |
| | Add video | + video |
| Audio/Video | | audio + video |
| | Negotiated down to audio during join | - video |
| | Add web[4] | + web |
| | Add video | + video |
| | Negotiated down to audio due to resource (BW) issue | - video |
| | Change Avaya Media Server from IVR to a different host or cascading | no change |
| Video only | | audio + video |
| Drop web[5] | | - web |
| Drop video | | - video |
| Drop audio/video | | - audio and - video |
| Hold/Resume – Mute/Unmute | | no change |
| Association (of two sessions) | | no change |
| Dis-association | | no change |

### Related links

How licensing works on page 160

## Licensing for Turnkey deployments

In a Turnkey deployment, the WebLM server is embedded in the Avaya Aura® Conferencing application.

[4] Login to Collaboration Agent or join to a web conference using Avaya Communicator or join a web conference using the mobile client.

[5] Logout from Collaboration Agent or logout from Web conferencing using Avaya Communicator or logout from Web conferencing using a mobile client.

**Related links**

Applying a license key on page 164
Backing up WebLM on page 164
Changing the administrator password for WebLM on page 165
Changing the certificate for WebLM on page 166
Installing WebLM on page 166
Resetting the administrator password for WebLM on page 167
Restoring WebLM on page 167
Starting a WebLM service on page 169
Stopping a WebLM service on page 169
Uninstalling WebLM on page 170
Upgrading WebLM on page 170

## Applying a license key

### Before you begin

Install the WebLM server. For more information, see Installing WebLM on page 166.

### About this task

Use these steps to apply a license for a Turnkey deployment.

### Procedure

1. Open the Weblm link `https://<primary EM host address>:12108/WebLM/`
2. Enter an administrator login and password.

   The default values for login and password are `admin` and `weblmadmin`.
3. Click **Log On** .
4. Select **Install license** from the left menu.
5. Click **Browse**.
6. Select a license file in XML format and click **Open**.
7. Click **Install**.

**Related links**

Licensing for Turnkey deployments on page 163

## Backing up WebLM

### Before you begin

Install the WebLM server. For more information, see Installing WebLM on page 166.

### About this task

Use these steps to back up all of the WebLM server data to the archive of the primary Element Manager.

### Procedure

1. Log to primary Element Manager server as `ntappadm`.
2. Type `weblmBackup.pl`.
3. Type `Y` to confirm.

### Example

```
[ntappadm@server58 install]$ weblmBackup.pl
Do you want to backup "WebLM service" (Y/N)?[Y]: Y
Backuping WebLM service...
Backup file: /var/mcp/weblm_backup_09-30-13_16-37-01.tar.gz
Backuping WebLM service completed successfully
```

### Related links

Licensing for Turnkey deployments on page 163

## Changing the administrator password for WebLM

### Before you begin

Install the WebLM server. For more information, see Installing WebLM on page 166.

### About this task

Use these steps to change the administrator password for WebLM.

### Procedure

1. Open the Weblm link `https://<primary EM host address>:12108/WebLM/`
2. Enter an administrator login and password.
3. Click **Log On**.
4. Select **Change password** at the right top corner.
5. Enter the **Current Password**.
6. Enter the **New Password**.
7. Confirm the password at the **Confirm Password** field.
8. Click **Submit**.

### Related links

Licensing for Turnkey deployments on page 163

## Changing the certificate for WebLM

These steps describe how to change the certificate for WebLM. You can also use these steps to change the listening and shutdown ports, but Avaya does not recommend changing the listening and shutdown ports.

### Before you begin

Install the WebLM server. For more information, see Installing WebLM on page 166.

### About this task

Use these steps to change the certificate used to access embedded WebLM server using a web browser.

### Procedure

1. Log to primary Element Manager server as `ntappadm`.
2. Type `weblmMgmt.pl`.
3. Enter a path to new certificate.
4. Enter a new password for certificate.
5. Choose a correct keystore format.
6. Type `Y` to confirm

### Example

```
[ntappadm@server58 install]$ weblmMgmt.pl
Path to certificate [/var/mcp/run/weblm/installed/certificate/
weblmserver.p12]: /var/mcp/install/weblm.jks
Certificate password [password]: RAPtor1234
Format keystore (JKS, PKCS11 or PKCS12) [PKCS12]: JKS
Tomcat listening port [12108]:
Tomcat shutdown port [12109]:
Do you want to configure "WebLM service" (Y/N)?[Y]: Y
Configuring WebLM service...
Configuring WebLM service completed successfully
```

**Related links**

Licensing for Turnkey deployments on page 163

## Installing WebLM

### About this task

Use these steps to install WebLM.

### Procedure

1. Log to primary Element Manager server as `ntappadm`.
2. Type `weblmInstall.pl`.

3. Select weblm load.
4. Type `Y` to confirm.

### Example

```
[ntappadm@server58 install]$ weblmInstall.pl
The following webLM application load instances have been found:
[1] /var/mcp/weblm_v6.3.3.5.8255_Tomcat_7.0.30.zip
[2] /var/mcp/weblm_v6.3.3.5.8255_tomcat_v7.0.30.zip
Please select which weblm load you wish to install [1..2]: 2
Do you want to install "WebLM service" (Y/N)?[Y]: Y
Installing WebLM service...
Installation of WebLM service completed successfully
```

**Related links**

Licensing for Turnkey deployments on page 163

## Resetting the administrator password for WebLM

### Before you begin

Install the WebLM server. For more information, see Installing WebLM on page 166.

### About this task

Use these steps to reset the administrator password for WebLM.

### Procedure

1. Log to primary Element Manager server as `ntappadm`.
2. Type `weblmResetAdminPwd.pl`.
3. Type `Y` to confirm.

### Example

```
[ntappadm@server58 install]$ weblmResetAdminPwd.pl
WARNING: All configured users for WebLM service will be lost!
Do you want to reset password for WebLM admin (Y/N)?[Y]:Y
Resetting password for WebLM admin...
Reset password for WebLM admin completed successfully
```

**Related links**

Licensing for Turnkey deployments on page 163

## Restoring WebLM

### Before you begin

Back up the WebLM server. For more information, see Backing up WebLM on page 164.

### About this task

Use these steps to restore the WebLM data from the archive.

## Procedure

1. Log to primary Element Manager server as `ntappadm`.

   There are three ways to use the `weblmRestore.pl` script.

2. **(Optional)** Method One:

   a. Type `weblmRestore.pl` to view a list of available files from the default directory (`/var/mcp/media/`).

   b. Choose the file you want to restore or use the Quit option to exit.

   c. If you want to restore WebLM service, type `Y` to confirm.

3. **(Optional)** Method Two

   a. Type `weblmRestore.pl -d` *`<the directory with backup files>`* to view a list of available files from the directory with backup files.

   b. Choose the file you want to restore or use the Quit option to exit.

   c. If you want to restore WebLM service, type `Y` to confirm.

4. **(Optional)** Method Three

   a. Type `weblmRestore.pl -f` *`<the full name to backup files>`*.

   b. The WebLM service is restored.

### Example

Example of method one:

```
ntappadm@server118 ~]$ weblmRestore.pl

Select backup file you want to restore

  [1] weblm_backup_06-19-14_14-03-17.tar.gz

  [2] weblm_backup_06-19-14_14-03-23.tar.gz

  [3] Quit


Please enter number [1 to 3] of selection:1

Do you want to restore "WebLM service" (Y/N)?[Y]: y

Restoring WebLM service...

Restoring WebLM service completed successfully
```

Example of method two:

```
2) [ntappadm@server118 ~]$ weblmRestore.pl -d /var/mcp


Select backup file you want to restore

  [1] weblm_backup_06-19-14_13-45-29.tar.gz
  [2] weblm_backup_06-19-14_14-03-40.tar.gz

  [3] Quit



Please enter number [1 to 3] of selection:1

Do you want to restore "WebLM service" (Y/N)?[Y]: y

Restoring WebLM service...

Restoring WebLM service completed successfully
```

Example of method three:

```
[[ntappadm@server118 ~]$ weblmRestore.pl -f /var/mcp/
weblm_backup_06-19-14_14-03-40.tar.gz

Restoring WebLM service...

Restoring WebLM service completed successfully
```

**Related links**

Licensing for Turnkey deployments on page 163

# Starting a WebLM service

## Before you begin

Install the WebLM server. For more information, see Installing WebLM on page 166.

## About this task

Use these steps to start the WebLM service.

## Procedure

1. Log to the primary Element Manager server as `root`.
2. Type `service weblm start`.

## Example

```
[root@server58 ~]# service weblm start
Starting WebLM service:                                    [  OK  ]
```

**Related links**

Licensing for Turnkey deployments on page 163

# Stopping a WebLM service

## Before you begin

Install the WebLM server. For more information, see Installing WebLM on page 166.

### About this task

Use these steps to stop the WebLM service.

### Procedure

1. Log to the primary Element Manager server as `root`.
2. Type `service weblm stop`.

### Example

```
[root@server58 ~]# service weblm stop
Stopping WebLM service:                                    [  OK  ]
```

### Related links

Licensing for Turnkey deployments on page 163

## Uninstalling WebLM

### Before you begin

Install the WebLM server. For more information, see Installing WebLM on page 166.

### About this task

Use these steps to remove WebLM from the primary Element Manager server.

### Procedure

1. Log to primary Element Manager server as `ntappadm`.
2. Type `weblmUninstall.pl`.
3. Type `Y` to confirm.

### Example

```
[ntappadm@server58 install]$ weblmUninstall.pl
Do you want to uninstall "WebLM service" (Y/N)?[Y]:
Uninstalling WebLM service...
WebLM service uninstalled successfully
```

### Related links

Licensing for Turnkey deployments on page 163

## Upgrading WebLM

### Before you begin

Copy the new WebLM load to the `/var/mcp` directory folder on the primary Element Manager server.

### About this task

Use these steps to upgrade WebLM to a new version.

### Procedure

1. Log to primary Element Manager server as `ntappadm`.
2. Type `weblmUpgrade.pl`.
3. Select weblm load.
4. Type `Y` to confirm.

### Example

```
[ntappadm@server58 install]$ weblmUpgrade.pl
The following webLM application load instances have been found:
[1] /var/mcp/weblm_v6.3.3.5.8220_Tomcat_7.0.29.zip
[2] /var/mcp/weblm_v6.3.3.5.8255_tomcat_v7.0.30.zip
Please select weblm load you wish to use for upgrade [1..2]: 2
Do you want to upgrade "WebLM service" (Y/N)?[Y]: y
Upgrading WebLM service...
Backup file: /var/mcp/weblm_backup_09-30-13_16-42-30.tar.gz
Upgrade of WebLM service completed successfully
```

**Related links**

Licensing for Turnkey deployments on page 163

## Licensing for Avaya Aura® deployments

In an Avaya Aura® deployment, Avaya Aura® System Manager hosts the WebLM server.

**Related links**

Installing the Avaya Aura Conferencing license key on Avaya Aura System Manager on page 171

## Installing the Avaya Aura® Conferencing license key on Avaya Aura® System Manager

### About this task

License keys are installed on the WebLM server, which resides with Avaya Aura® System Manager. WebLM has a client/server model where many clients share the same WebLM server and also the same license key. The license key is an XML file.

Use the following procedure to install the Avaya Aura® Conferencing license key on Avaya Aura® System Manager.

### Procedure

1. In the Address box of the Web browser, enter the following address: `http://<SMGR OAM FQDN>`.
2. In the User ID field, enter your System Manager logon ID.
3. In the Password field, enter your password.

4. Click **Log On**.
5. In the Services area of the System Manager home page, click **Licenses**.
6. In the navigation pane, click **Install license**.
7. On the Install license page, click **Browse**.
8. In the Choose File to Upload dialog box, select the license file, and click **Open**.
9. Click **Install**.
10. In the navigation pane, click **Conferencing** to view information about the license.

**Related links**

Licensing for Avaya Aura deployments on page 171

# Chapter 9: Installing Avaya Aura® Conferencing (AAC) for Avaya Aura® using VMWare

## Introduction to vAAC

Virtualization is becoming more prevalent within enterprise business data centers and is seen as a way to reduce both capital expenditure (capex) and total cost of ownership (TCO). VMware™ is a leader in virtualization technology and seen as an important platform for Avaya to adopt for its enterprise solutions. VMware provides centralized management of virtualized hosts and virtual machines from a single console. It provides a comprehensive suite of tools to help the administrator monitor and manage their data center.

The Avaya Aura® Conferencing on VMware feature creates images with pre-configured and fully functional Avaya Aura® Conferencing software which is packaged in the standard template format (OVA - Open Virtualization Achive) for deploying into the customer's VMware virtual infrastructure. Avaya refers to the virtualized Avaya Aura® Conferencing solution as "vAAC".

In this release, multiple OVAs support the various deployment scenarios:

- vAAC Medium Simplex OVA: AAC RHEL platform + Pre-installed/deployed/configured application bundle (EM, DB, PROV, WCMS, WCS, AS, AMS, AM, DCS, FMG)
    - All NEs are deployed & started automatically.
- vAAC Medium Redundant Primary OVA: AAC RHEL platform + Pre-installed/deployed/configured Medium Primary application bundle (EM, DB, PROV, WCMS, WCS, AS, AMS, AM, DCS, FMG)
    - All NEs (on Primary instances) are deployed & started automatically.
- vAAC Medium Redundant Secondary OVA: AAC RHEL platform + Pre-installed/deployed/configured medium secondary application bundle (EM, DB, PROV, WCMS, WCS, AS, AMS, AM, DCS, FMG)
    - All NEs are deployed & started automatically.
- vAAC Platform: AAC RHEL platform + Application Bundle ISO file.
    - Avaya Aura® Conferencing platform is installed and started.
    - Admin has to run "mcpInstaller" to install AAC NEs.
    - During the vAAC Platform OVA deployment, you, as the customer, can select large platform resources or small platform resources.

**Note:**

VMware is only supported on medium and large deployments and is not supported on SMB deployments.

**Note:**

Use of vMotion for automatic disaster recovery (ADR) is not supported. Instead, you must use the ADR feature of Avaya Aura® Conferencing.

### Flexible deployment: Large platform resources or small platform resources

For this release, Avaya created two platform OVAs (vAAC_LargePlatform and vAAC_SmallPlatform):

- vAAC_LargePlatform OVA's vCPU and memory resources: 12 vCPUs (100% reserved), 30 GB Memory (100% reserved)
- vAAC_SmallPlatform OVA's vCPU and memory resources: 6 vCPUs (100% reserved), 16 GB Memory (100% reserved)

With the exception of the OVA vCPU and memory resource configuration and reservation, all other parameters were the same for these OVAs. These two OVAs were two different entities, which the customer had to download.

For this release, Avaya simplified the two platform OVAs by introducing a flexible deployment feature. Now, there is a single platform OVA. During the platform OVA deployment, the wizard prompts customers to select the deployment configuration. There are two deployment configuration options:

- Large Platform Resources
- Small Platform Resources

With this feature, customers can choose difference resource configuration during the OVA deployment. The Large Platform Resources option is compatible with the Large Platform OVA deployment from previous releases. The Small Platform Resources option is compatible with the Small Platform OVA deployment from previous releases.

The Avaya Aura® Conferencing software will now be supported in VMWare environments that utilize the ESXi 5.1, ESXi 5.5, and ESXi 6 hypervisors. Avaya will provide virtual machine templates called OVA files. These files specify the required number of virtual CPUs, memory, disk space, and disk performance required by the VM. .

### OVA deployment model summary

The following table shows the number of OVAs that are required to deploy each of the deployment models. These are the minimum number of virtual machines (VMs) that are required as per the staging files.

**Note:**

A solution may add additional VMs (using the vAAC Platform OVA) as required, supporting additional optional components.

| OVAs required per deployment | vAAC-Medium Simplex OVA | vAAC-Medium Redundant Primary OVA | vAAC-Medium Redundant Secondary OVA | vAAC-Platform OVA<br>(with Large Platform Resources Deployment Option) | vAAC-Platform OVA<br>(with Small Platform Resources Deployment Option) |
|---|---|---|---|---|---|
| Medium Simplex | 1 | | | | 0 to 10 (cascading Avaya Aura® Media Server (MS)s) |
| Medium Redundant | | 1 | 1 | | 0 to 10 (cascading Avaya Aura® Media Server (MS)s) |
| Large Simplex (starting configuration) | | | | 3 | 0 to 32 (cascading Avaya Aura® Media Server (MS)s) |
| Large Redundant (starting configuration) | | | | 6 | 0 to 32 (cascading Avaya Aura® Media Server (MS)s) |
| Large Redundant (expansion) | | | | 8 | 2 Document Conversion Servers (DCS)<br>0 to 32 Avaya Aura® Media Server (MS)s |

**Note:**

Currently, Avaya Aura® Conferencing does not support VMware for the SMB-sized solution. You can only using VMware for medium or large deployments.

## OVA resource reservation requirements

| AAC OVA | Processor<br>vCPUs | Processor<br>Reservation<br>(MHz) | Memory<br>(GB) | Memory reservation (GB) | Disk size<br>(GB) | Physical cores<br>Minimum frequency |
|---|---|---|---|---|---|---|
| Medium Simplex OVA | 8 | 23,144 | 24 | 24 | 150 | 2,893 |

*Table continues…*

| AAC OVA | Processor<br>vCPUs | Processor<br>Reservation<br>(MHz) | Memory<br>(GB) | Memory reservation (GB) | Disk size<br>(GB) | Physical cores<br>Minimum frequency |
|---|---|---|---|---|---|---|
| Medium Redundant Primary OVA | 8 | 23,144 | 24 | 24 | 150 | 2,893 |
| Medium Redundant Secondary OVA | 8 | 23,144 | 24 | 24 | 150 | 2,893 |
| Platform Large Footprint OVA | 12 | 34,716 | 30 | 30 | 150 | 2,893 |
| Platform Small Footprint OVA | 6 | 17,358 | 16 | 16 | 150 | 2,893 |

**Note:**

For medium systems, eight vCPU and 24 GB memory will only support 2000 user capacity. To support 5000 user capacity, you must increase resources to 12 vCPU, 30 GB. You must use the following procedure to update the resource reservation. For more information, see Modifying vAAC OVA resource reservation and the number of CPUs on page 193.

## Cascading capacity

The following table shows the supported capacity for cascading Avaya Aura® Media Servers for Avaya Aura® Conferencing.

| | Capacity (Audio Sessions) | Capacity (Video Sessions) | CPUs | Memory (GB) | Storage (GB) | CPU Speed (GHZ) | CPU Reservation (GHZ) |
|---|---|---|---|---|---|---|---|
| VMware system:<br>Cascading Avaya Aura® Media Servers (6 vCPUs) | 540 | 160 | 6 | 16 | 150 | 2.893 | 17.358 |
| Bare-metal system:<br>Cascading Avaya Aura® Media Servers | 600 | 180 | 6 | 16 | 150 | 6 (12 with hyperthreading) | N/A |

**Related links**

Modifying the vAAC OVA resource reservation and the number of CPUs on page 193

## Checklist for installing the AAC Avaya Aura® solution

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Ensure that you are qualified to perform this task. | Ensure that you have the skills required to install, configure, and upgrade Avaya Aura® Conferencing. For a list of the required core competencies, see Audience on page 26. Before undertaking any advanced procedures, you must complete the required Avaya Aura® Conferencing training, as listed in Training on page 23. Avaya recommends that you download all available Avaya Aura® Conferencing documentation, as listed in Documentation on page 20. | | |
| 2 | Read the prerequisites | Prerequisities to running vAAC OVAs on page 178 | | |
| 3 | Deploy the OVAs | Deploying vAAC OVAs on page 179 | | |
| 4 | Configure the platform | Configuring the vAAC platform after the OVA deployment on page 180 | | |
| 5 | Configure for your specific deployment type | If you have a medium deployment without redundancy, see Configuring a vAAC medium simplex system after the OVA deployment on page 182<br>If you have a medium deployment with redundancy, see | | |

*Table continues…*

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| | | Configuring a vAAC medium redundant primary system after the OVA deployment on page 186 and Configuring a vAAC medium redundant secondary core server after the OVA deployment on page 190<br>If you have a large deployment with redundancy, see Installing the components for Avaya Aura® Conferencing on page 132. | | |
| 6 | Perform a number of provisioning tasks to enable you to place a test call to verify the installation. | Read the following section for guidance: Deciding the next steps on page 196 | | |

## Prerequisites to running vAAC OVAs

- You must install ESXi hypervisor. ESXi hypervisor is required on physical hosts for virtualizing resources such as, CPUs, RAMs, NICs and storage. On the ESXi hypervisor, you must ensure that **Hyperthreading** is set to **Active**.
  - vSphere client is the administrative tool for managing ESXi hosts.
  - vCenter server is the management server, through which ESXi resources pools, and other VMware advanced features can be managed or enabled by vSphere client.
  - vMotion is a component of vSphere that allows the live migration of a running virtual machine's (VM) file system from one storage system to another. If you are using vMotion, you must take the network element out of service first. Use of vMotion for automatic disaster recovery (ADR) is not supported. Instead, you must use the ADR feature of Avaya Aura® Conferencing.
- You can create virtual machines on shared storage — in other words, iSCSI NAS (Network Attached Storage), or local attached storage.

  **Note:**

  The virtual machines have no knowledge of the underlying physical disks. All virtual disks will appear to be SCSI disk drive to virtual machines.

# Deploying vAAC OVAs

Each of the following procedures use VMware vSphere PC client and connects to VMware vCenter. The current procedure applies to all vAAC OVA deployment models.

## Before you begin

Download all required vAAC OVA files to your computer before you begin.

## About this task

Use this task to deploy vAAC OVAs to the VMware Virtual Machine (VM).

## Procedure

1. Login to the vCenter through vSphere PC client.
2. Select a target EXSi host from **vSphere Client** > **Hosts and Clusters view**.
3. Click **File** > **Deploy OVF Template...**.

   The **Deploy OVF Template** wizard begins.
4. At the **Source** step, select the vAAC OVA file from your computer and click **Next**.
5. At the **OVF Template Details** step, display the select OVA file information and click **Next**
6. At the **End User License Agreement** step, read the license agreement, click **Accept** and click **Next**.
7. At the **Name and Location** step, enter a proper VM name and select a proper data center in the **Inventory Location** and click **Next**.
8. At the **Deployment Configuration** step, select the **Large Platform Resources** or the **Small Platform Resources** option and click **Next**

   **Note:**

   If you are deploying the non-platform OVAs, you can skip this step.
9. At the **Storage** step, select the proper storage to which you want to deploy the OVA and click on **Next**.
10. At the **Disk Format** step, select **Thick Provision Lazy Zeroed** and click **Next**.
11. At the **Ready to Complete** step, verify the information and click **Finish**.

    The **VM deployment progress** dialog is displayed
12. After the VM is successfully deployed, select the VM, right click on it, and select **Power** > **Power On**.

## Result

The selected vAAC OVA has been deployed and powered on.

## Next steps

Proceed to Configuring the vAAC platform after the OVA deployment on page 180.

## Configuring the vAAC platform after the OVA deployment

The attribute selections in this procedure reflect a particular example configuration. Your configuration may differ and as such, may require different attribute selections.

### Before you begin

Enter the IP addresses and Fully Qualified Domain Names (FQDN) of each of the server resources in the following table. You will require this information during the configuration.

| Resource Name | IP Address | FQDN |
|---|---|---|
| Primary Element Manager Server | | |
| Element Manager Service | | |
| Accounting Manager Service | | |
| Application Server Service | | |
| Primary Media Server Media Address | | |
| Primary Web Conferencing Server Service | | |
| NTP Server | | |
| DNS Server | | |
| Gateway/Subnet address[6] | | |
| System Manager (SMGR)[6] | | |
| Session Manager (SM) SIP[6] | | |

### About this task

Use this task to configure the vAAC platform after the OVA deployment. This task applies to vAAC Platform Large Platform and Small Platform deployments.

**Tip:**

In order to progress through the VM Console, you can click **Ctrl + Alt + left click**.

### Procedure

1. Right click on the VM and select **Open Console**.
2. On the Hostname Configuration screen, type the hostname and press **Enter**.
3. At the confirmation prompt, type `Y` and press **Enter**.

   The Network Configuration screen is displayed.
4. Configure the network, as follows:
   a. At the **Enter IP address** prompt, type the *Primary EM Server IP Address* from the table above.

[6] Not required for Turnkey.

   b. At the **Enter subnet prefix length (1–38)** prompt, type the appropriate alphanumeric length.
   c. At the **Enter gateway IP address** prompt, type the *Gateway address* from the table above.
   d. At the confirmation prompt, type **Y** and press **Enter**.

      The DNS Configuration screen is displayed.

5. Configure the DNS, as follows:
   a. At the **Domain Suffix(es): Enter Selection** prompt, accept the default configuration by typing `C`.
   b. At the **How many DNS Servers would you like to reference (1–3)** prompt, type the appropriate number, such as `1`.
   c. At the **Enter Primary DNS Server (<DNS server IP address>)** prompt, type the DNS IP address.
   d. At the confirmation prompt, type `Y` and press **Enter**.

      The Configuration Confirmation screen is displayed.
   e. Type `Y` and press **Enter**.

      The Configuration Confirmation screen for the timezone is displayed.
6. Configure the timezone, as follows:
   a. At the **Use the default value (US/Eastern) for this timezone** prompt, type **Y** to use default value or type **N** to reconfigure the timezone.
   b. At the confirmation prompt, type `Y` and press **Enter**.

      The Date and Time screen is displayed.
7. Configure the date and time as follows:
   a. At the **Do you want to keep this date and time (Y/N) [Y]?** prompt, type **Y** to use current date and time or type **N** to reconfigure the date and time.
   b. At the confirmation prompt, type **Y** and press **Enter**.

   The NTP Configuration screen is displayed.
8. Configure the NTP server. For more information, see Configuring the NTP clock on page 127.
9. Configure the SysLog server details, as follows:
   a. At the **Do you wish to configure/unconfigure/display the SysLog Server IP Address?** prompt, type `u`.
   b. At the confirmation prompt, type `Y` and press **Enter**.

      The Encrypt Recording Data Disk screen is displayed.

10. Configure encryption of the recording data disk, as follows:
    a. At the **Do you wish to encrypt the recording data disk? (Y/N) [N]?** prompt, type **N** to use the default non-encryption for the recording data disk, then press **Enter** to continue. Alternatively, you can type **Y** to configure the recording data disk encryption.
    b. To configure encryption, type Y and enter a phrase in the **Enter the encryption secure phrase** and **Enter the encryption secure phrase again** fields.
    c. At the confirmation prompt, type `Y` and press **Enter**.
11. Press **Enter** to finish.

### Result

The vAAC platform is configured.

### Next steps

It is a good idea to back up the platform at this point.

⚠ **Warning:**

After the installation, you need to provide a platform back-up. If you do not back up the platform then during the platform failure, all information on the recording data disk is lost. There is no other way to restore or recreate the encrypted secure phrase.

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

## Configuring a vAAC medium simplex system after the OVA deployment

The attribute selections in this procedure reflect a particular example configuration. Your configuration may differ and as such, may require different attribute selections.

This example is for an Avaya Aura® deployment. If yours is a Turnkey deployment, see Configuring a vAAC medium simplex system after the OVA deployment on page 209.

### Before you begin

- Enter the IP addresses and Fully Qualified Domain Names (FQDN) of each of the server resources in the following table. You will require this information during the configuration.

| Resource Name | IP Address | FQDN |
|---|---|---|
| Primary Element Manager Server | | |
| Element Manager Service | | |
| Accounting Manager Service | | |

*Table continues…*

| Resource Name | IP Address | FQDN |
|---|---|---|
| Application Server Service | | |
| Primary Media Server Media address | | |
| Primary Web Conferencing Server Service | | |
| Primary Provisioning Manager | Same as Primary Element Manager Server IP | |
| Primary Web Collaboration Agent Manager | Same as Primary Element Manager Server IP | |
| Primary Document Conversion Server | Same as Primary Element Manager Server IP | |
| FMG (Flash Media Gateway) Server | | |
| NTP Server | | |
| DNS Server | | |
| Gateway/Subnet address | | |
| System Manager (SMGR) | | |
| System Manager (SMGR) enrollment password | | |
| Session Manager (SM) SIP | | |

- Complete the steps in Configuring the vAAC platform after the OVA deployment on page 180.

## About this task

Use this task to configure a vAAC medium simplex deployment.

**Tip:**

In order to progress through the VM Console, you can click **Ctrl + Alt + left click**.

## Procedure

1. If this is the Avaya Aura® configuration, please select option 1: AAC with Avaya Aura® on the Avaya Aura® Conferencing System Deployment Type Configuration screen.
2. On the Avaya Aura® Conferencing Core Application Configuration screen, configure the core application IP addresses, as follows:
    a. At the **Please enter the Service IPv4 address of Element Manager** prompt, enter the *EM Service IP* address from the table above.
    b. At the **Please enter the Service IPv4 address of Accounting Manager** prompt, enter the *Accounting Manager Service IP* from the table above.
    c. At the **Please enter the Service IPv4 address of Application Server** prompt, enter the *Application Server IP* from the table above.
    d. At the **Please enter the Media IPv4 address of the primary media server** prompt, enter the *Primary Media Server IP* from the table above.

e. At the **Please enter the Service IPv4 address of the primary Web Conferencing Server** prompt, enter the *Primary WCS Service IP* from the table above.

f. At the **Please enter the FQDN for the Service address of the Element Manager** prompt, enter the Service address of the Element Manager FQDN from the table above.

g. At the **Please enter the FQDN for the primary Provisioning Manager** prompt, enter the primary *Provisioning Manager FQDN* from the table above.

h. At the **Please enter the FQDN for the primary Web Conferencing Server** prompt, enter the primary *Web Conferencing Server FQDN* from the table above.

i. At the **Please enter the FQDN for the primary Collaboration Agent Manager** prompt, enter the *primary Collaboration Agent Manager FQDN* from the table above.

j. At the **Please enter the FQDN for the primary Document Conversion Server** prompt, enter the primary *Document Conversion Server FQDN* from the table above.

k. At the **Please enter the Site Name of this AAC installation** prompt, enter a short name for the site you are configuring.

l. At the **Please enter the Site Long Name of this AAC installation** prompt, enter a longer name for the site you are configuring.

3. On the Flash Media Gateway (FMG) Configuration screen, configure the FMG as follows:

a. At the **Enter the IP address for JMX Connections** prompt, type the *FMG Server IP address* from the table above.

b. At the **Enter the IP address for RTMP Connections** prompt, type the *FMG Server IP address* from the table above.

c. At the **Enter the IP address for HTTP Connections** prompt, type the *FMG Server IP address* from the table above.

d. At the **Enable RTMPS?** prompt, type `yes`.

e. At the **Enter the Port for RTMPS** prompt, enter the port number for RTMPS connections.

f. At the **Generate a self-signed certificate for RTMPS (Port 443)** prompt, type `yes`.

g. At the **Enable RTMP?** prompt, type `yes`.

h. At the **Enter the Port for RTMP** prompt, type `1935`.

i. At the **Enable RTMPT?** prompt, type `yes`.

j. At the **Enter the Port for RTMPT** prompt, type `80`.

k. In the **Management Configuration** section, at the **Enter the IP address for Management Client** prompt, type the *FMG Server IP address* from the table above.

l. At the **Enter the Port for Management Client** prompt, enter the port number for management client connections.

m. At the **Generate a self-signed certificate for RTMPS for Management Portal** prompt, type `yes`.

The FMG is configured.

4. Configure the Avaya Aura® servers, as follows:
    1. At the **Please enter the IPv4 address of the Aura System Manager** prompt, enter the *System Manager IP* from the table above.
    2. At the **Please enter the IPv4 address of Aura Session Manager** prompt, enter the *Session Manager SIP IP* from the table above.
    3. At the **Please enter the FQDN for the Aura System Manager** prompt, enter the *Aura System Manager FQDN* from the table above. During the OVA configuration phase, the VM network configuration is not up and running so the OVA configuration implementation cannot verify the entered FQDN value. The WARNING message will be displayed as **WARNING: FQDN does not resolve to address: mySystemManager.com. Do you want to change value? (Y/N)? [Y]**. Please enter **N** to use the entered FQDN configuration.
    4. At the **Please enter the SMGR SNMP Trap Listener Port for Alarm Forwarding** prompt, enter the port number for alarm connections.
    5. At the **Please enter the SMGR SNMP Community String (for Alarm forwarding)** prompt, enter the appropriate community string, such as `public`, for alarms.

       The vAAC progresses through an initial configuration phase.
5. When this configuration is complete, you can configure the enrollment password, as follows:
    1. At the **Please enter the Enrollment Password** prompt, the *System Manager Enrollment password* from the table above.
    2. At the **Please reenter the Enrollment Password** prompt, enter the enrollment password again.
    3. At the **Does the Thumbprint above match the Thumbprint of the Avaya Aura System Manager Certificate Authority** prompt, verify the thumbprint and enter **Y**.
6. At the **Press ENTER to reboot the vAAC to complete OVA configuration...** prompt, press **Enter** to reboot the vAAC.

## Result

The vAAC Medium Simplex system is configured.

## Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

# Configuring a vAAC medium redundant primary core server after the OVA deployment

### Before you begin

- Enter the IP addresses and Fully Qualified Domain Names (FQDN) of each of the server resources in the following table. You will require this information during the configuration.

| Resource Name | IP Address | FQDN |
|---|---|---|
| Primary Element Manager Server | | |
| Secondary Element Manager Server | | |
| Element Manager Service | | |
| Accounting Manager Service | | |
| Application Server Service | | |
| Primary Media Server Media address | | |
| Secondary Media Server Media address | | |
| Primary Web Conferencing Server (WCS) Service | | |
| Primary Provisioning Manager | Same as Primary Element Manager Server IP | |
| Secondary Provisioning Manager | Same as Secondary Element Manager Server IP | |
| Primary Web Collaboration Agent Manager | Same as Primary Element Manager Server IP | |
| Secondary Web Collaboration Agent Manager | Same as Secondary Element Manager Server IP | |
| Primary Document Conversion Server | Same as Primary Element Manager Server IP | |
| Secondary Document Conversion Server | Same as Secondary Element Manager Server IP | |
| Secondary Web Conferencing Server (WCS) Service | | |
| FMG Server IP on Primary | | |
| NTP Server | | |
| DNS Server | | |
| Gateway/Subnet address | | |
| System Manager (SMGR) | | |

*Table continues…*

| Resource Name | IP Address | FQDN |
|---|---|---|
| System Manager (SMGR)<br>Enrollment password | | |
| Session Manager (SM) SIP | | |

- Complete the steps in Configuring the vAAC platform after the OVA deployment on page 180.

### About this task

Use this task to configure a vAAC medium redundant primary core server.

### Procedure

1. If this is the Avaya Aura® configuration, please select option 1: AAC with Avaya Aura® on the Avaya Aura® Conferencing System Deployment Type Configuration screen.
2. On the Avaya Aura® Conferencing Core Application Configuration screen, configure the core application IP addresses, as follows:
    a. At the **Please enter the Internal OAM (Default) IPv4 address of the secondary Element Manager server** prompt, enter the *Secondary Element Manager Server* address from the table above.

    b. At the **Please enter the Service IPv4 address of Element Manager** prompt, enter the *EM Service IP* address from the table above.

    c. At the **Please enter the Service IPv4 address of Accounting Manager** prompt, enter the *Accounting Manager Service IP* from the table above.

    d. At the **Please enter the Service IPv4 address of Application Server** prompt, enter the *Application Server IP* from the table above.

    e. At the **Please enter the Media IPv4 address of the primary media server** prompt, enter the *Primary Media Server IP* from the table above.

    f. At the **Please enter the Media IPv4 address of the secondary media server** prompt, enter the *Secondary Media Server IP* from the table above.

    g. At the **Please enter the Service IPv4 address of the primary Web Conferencing Server** prompt, enter the *Primary WCS Service IP* from the table above.

    h. At the **Please enter the Service IPv4 address of the secondary Web Conferencing Server** prompt, enter the *Secondary WCS Service IP* from the table above.

    i. At the **Please enter the FQDN for the Service address of the Element Manager** prompt, enter the *Service address of the Element Manager FQDN* from the table above.

    j. At the **Please enter the FQDN for the primary Provisioning Manager** prompt, enter the *Primary Provisioning Manager FQDN* from the table above.

    k. At the **Please enter the FQDN for the secondary Provisioning Manager** prompt, enter the *Secondary Provisioning Manager FQDN* from the table above.

    l. At the **Please enter the FQDN for the primary Web Conferencing Server** prompt, enter the *Primary Web Conferencing Server FQDN* from the table above.

m. At the **Please enter the FQDN for the secondary Web Conferencing Server** prompt, enter the *Secondary Web Conferencing Server FQDN* from the table above.

n. At the **Please enter the FQDN for the primary Collaboration Agent Manager** prompt, enter the *Primary Collaboration Agent Manager FQDN* from the table above.

o. At the **Please enter the FQDN for the secondary Collaboration Agent Manager** prompt, enter the *Secondary Collaboration Agent Manager FQDN* from the table above.

p. At the **Please enter the FQDN for the primary Document Conversion Server** prompt, enter the *Primary Document Conversion Server FQDN* from the table above.

q. At the **Please enter the FQDN for the secondary Document Conversion Server** prompt, enter the *Secondary Document Conversion Server FQDN* from the table above.

r. At the **Please enter the Site Name of this AAC installation** prompt, enter a short name for the site you are configuring.

s. At the **Please enter the Site Long Name of this AAC installation** prompt, enter a longer name for the site you are configuring.

t. Press **Enter** to continue.

3. On the Flash Media Gateway (FMG) Configuration screen, configure the FMG as follows:

a. At the **Enter the IP address for JMX Connections** prompt, type the *FMG Server IP address* from the table above.

b. At the **Enter the IP address for RTMP Connections** prompt, type the *FMG Server IP address* from the table above.

c. At the **Enter the IP address for HTTP Connections** prompt, type the *FMG Server IP address* from the table above.

d. At the **Enable RTMPS?** prompt, type `yes`.

e. At the **Enter the Port for RTMPS** prompt, enter the port number for RTMPS connections.

f. At the **Generate a self-signed certificate for RTMPS (Port 443)** prompt, type `yes`.

g. At the **Enable RTMP?** prompt, type `yes`.

h. At the **Enter the Port for RTMP** prompt, type `1935`.

i. At the **Enable RTMPT?** prompt, type `yes`.

j. At the **Enter the Port for RTMPT** prompt, type `80`.

k. In the **Management Configuration** section, at the **Enter the IP address for Management Client** prompt, type the *FMG Server IP address* from the table above.

l. At the **Enter the Port for Management Client** prompt, enter the port number for management client connections.

m. At the **Generate a self-signed certificate for RTMPS for Management Portal** prompt, type `yes`.

The FMG is configured.

4. Configure the Avaya Aura® servers, as follows:
    a. At the **Please enter the IPv4 address of the Aura System Manager** prompt, enter the *System Manager IP* from the table above.
    b. At the **Please enter the IPv4 address of Aura Session Manager** prompt, enter the *Session Manager SIP IP* from the table above.
    c. At the **Please enter the FQDN for the Aura System Manager** prompt, enter the *Aura System Manager FQDN* from the table above. During the OVA configuration phase, the VM network configuration is not up and running so the OVA configuration implementation cannot verify the entered FQDN value. The WARNING message will be displayed as **WARNING: FQDN does not resolve to address: mySystemManager.com. Do you want to change value? (Y/N)? [Y]**. Please enter **N** to use the entered FQDN configuration.
    d. At the **Please enter the SMGR SNMP Trap Listener Port for Alarm Forwarding** prompt, enter the port number for alarm connections.
    e. At the **Please enter the SMGR SNMP Community String (for Alarm forwarding)** prompt, enter the appropriate community string for alarms.

    The vAAC progresses through an initial configuration phase.
5. When this configuration is complete, you can configure the enrollment password, as follows:
    a. At the **Please enter the Enrollment Password** prompt, the *System Manager Enrollment password* from the table above.
    b. At the **Please reenter the Enrollment Password** prompt, enter the enrollment password again.
    c. At the **Does the Thumbprint above match the Thumbprint of the Avaya Aura System Manager Certificate Authority** prompt, verify the thumbprint and enter **Y**.
6. At the **Press ENTER to reboot the vAAC to complete OVA configuration...** prompt, press **Enter** to reboot the vAAC.

## Result

The vAAC medium redundant primary core server is configured.

## Next steps

Proceed to Configuring a vAAC medium redundant secondary core server after the OVA deployment on page 190.

# Configuring a vAAC medium redundant secondary core server after the OVA deployment

The table of IP addresses and FQDNs that you use in this task should contain the same information that you used in Configuring a vAAC medium redundant primary core server after the OVA deployment on page 186.

## Before you begin

- Enter the IP addresses and Fully Qualified Domain Names (FQDN) of each of the server resources in the following table. You will require this information during the configuration.

| Resource Name | IP Address | FQDN |
|---|---|---|
| Primary Element Manager Server | | |
| Secondary Element Manager Server | | |
| Element Manager Service | | |
| Accounting Manager Service | | |
| Application Server Service | | |
| Primary Media Server Media address | | |
| Secondary Media Server Media address | | |
| Primary Web Conferencing Server (WCS) Service | | |
| Primary Provisioning Manager | Same as Primary Element Manager Server IP | |
| Secondary Provisioning Manager | Same as Secondary Element Manager Server IP | |
| Primary Web Collaboration Agent Manager | Same as Primary Element Manager Server IP | |
| Secondary Web Collaboration Agent Manager | Same as Secondary Element Manager Server IP | |
| Primary Document Conversion Server | Same as Primary Element Manager Server IP | |
| Secondary Document Conversion Server | Same as Secondary Element Manager Server IP | |
| Secondary Web Conferencing Server (WCS) Service | | |
| FMG Server IP on Primary | | |
| NTP Server | | |

*Table continues…*

| Resource Name | IP Address | FQDN |
|---|---|---|
| DNS Server | | |
| Gateway/Subnet address | | |
| System Manager (SMGR) | | |
| System Manager (SMGR) Enrollment password | | |
| Session Manager (SM) SIP | | |

- Complete the steps in Configuring the vAAC platform after the OVA deployment on page 180.

## About this task

Use this task to configure a vAAC medium redundant secondary core server.

## Procedure

1. Configure the Avaya Aura® Conferencing Core Application only for Secondary, as follows:

   At the **Please enter the Internal OAM (Default) IPv4 address of the primary Element Manager server** prompt, enter the Primary EM Server IP address from the table above.

   The vAAC configuration automatically continues and displays a progress counter. When the configuration is complete, all network elements are up and running.

2. On the Flash Media Gateway (FMG) Configuration screen, configure the FMG as follows:

   a. At the **Enter the IP address for JMX Connections** prompt, type the *FMG Server IP address* from the table above.

   b. At the **Enter the IP address for RTMP Connections** prompt, type the *FMG Server IP address* from the table above.

   c. At the **Enter the IP address for HTTP Connections** prompt, type the *FMG Server IP address* from the table above.

   d. At the **Enable RTMPS?** prompt, type `yes`.

   e. At the **Enter the Port for RTMPS** prompt, enter the port number for RTMPS connections.

   f. At the **Generate a self-signed certificate for RTMPS (Port 443)** prompt, type `yes`.

   g. At the **Enable RTMP?** prompt, type `yes`.

   h. At the **Enter the Port for RTMP** prompt, type `1935`.

   i. At the **Enable RTMPT?** prompt, type `yes`.

   j. At the **Enter the Port for RTMPT** prompt, type `80`.

   k. In the **Management Configuration** section, at the **Enter the IP address for Management Client** prompt, type the *FMG Server IP address* from the table above.

   l. At the **Enter the Port for Management Client** prompt, enter the port number for management client connections.

m. At the **Generate a self-signed certificate for RTMPS for Management Portal** prompt, type `yes`.

   The FMG is configured.

3. The vAAC progresses through an initial configuration phase. The vAAC displays a progress counter.
4. The results are displayed in the VM Console window.
5. At the **Press ENTER to reboot the vAAC to complete OVA configuration...** prompt, press **Enter** to reboot the vAAC.

### Result

The configuration of the secondary server is complete.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

## Verifying and upgrading VMWare tools

### Before you begin

Ensure that the vAAC OVA is deployed on the VMWare host.

### About this task

Use this task to upgrade the VMWare tools package on the deployed vAAC OVAs.

### Procedure

1. Login to the vCenter using the vSphere PC client.
2. In **Hosts and Clusters** view, select a target vAAC VM from the vSphere client.
3. Navigate to **vAAC VM Summary** and verify whether the VMware Tools are **Current**.

   If the VMWare Tools are current, there is no need to upgrade them.
4. If the VMware Tools are **Out-of-Date**, use the right-click to navigate to **vAAC VM** > **Guest** > **Install/Upgrade VMWare Tools**.
5. Select **Automatic Tools Update** and click **OK**.

   The upgrade process takes approximate three to four minutes. The status panel displays **In Progress**.

### Result

After a successful upgrade, the **vAAC VM Summary** tab displays the VMWare Tools as **Current**. If the upgrade fails, you must manually install the VMware Tools package. See Manually installing the VMware tools package on page 194.

# Modifying the vAAC OVA resource reservation and the number of CPUs

For medium systems, eight vCPU and 24 GB memory will only support 2000 user capacity. To support 5000 user capacity, you must increase resources to 12 vCPU, 30 GB. You must use the following procedure to update the resource reservation. For more information, see Modifying vAAC OVA resource reservation and the number of CPUs on page 193.

### Before you begin

- Deploy a vAAC medium simplex OVA, a medium redundant primary OVA, a medium redundant secondary, a platform large footprint, or a platform small footprint OVA.
- Ensure that the VM is powered off.

### About this task

Use this task to modify OVA CPU and memory resources reservation and total number of CPUs for a deployed vAAC Virtual Machine (VM).

### Procedure

1. If the deployed vAAC VM has been powered on, power off the VM:

   In the vSphere client, right click on the vAAC VM and select **Power** > **Power Off**.
2. Right click on the VM and select **Edit Settings...** > **Edit Settings...**.
3. In the Edit Settings popup dialog, click on the **Resources** tab.
4. Change the CPU resource reservation:

   Select the CPU item in the left panel and enter the desired CPU reservation number (in MHz) in the **Reservation** field in the **Resource Allocation** panel
5. Change the memory resource reservation:

   Select the Memory item in the left panel and enter desired memory reservation number (in MB) in the **Reservation** field in the **Resource Allocation** panel
6. Click **OK** in the Edit Settings popup dialog.
7. Right click on the VM and select **Edit Settings...** > **Edit Settings...**.
8. In the Edit Settings popup dialog, click on the **Hardware** tab.
9. Change the total number of CPUs:
   a. Select the CPUs item in the left panel and select the desired virtual sockets at the **Number of virtual sockets** parameter drop-down list in right panel.
   b. Do not change the **Number of cores per socket** parameter value.
10. Click **OK** in the Edit Settings popup dialog.
11. Select the vAAC VM, right click on it and select **Power** > **Power On**.

### Related links

Introduction to vAAC on page 173

# Manually installing the VMware tools package

## Before you begin

The deployed vAAC VM must be powered on and running. It must have access to the current VMware host's datastore.

## About this task

Use this task to manually install a compatible VMware tools package to the deployed vAAC VM.

## Procedure

1. In vSphere Client, select the deployed VM, right-click on it and click **Edit Settings...**
2. In the **Edit Settings** popup window, on the **Hardware** tab, select **CD/DVD drive 1**.
3. From the **Device Type** panel, select **Datastore ISO File** and click **Browse...**
4. On the **Browse** dialog, navigate to **Datastores** > **vmimages** > **tools-isoimages** > **linux.iso**. Click **Open** on the **linux.iso** file.
5. In the **Edit Settings** popup window, in the **Device Status** panel, select **Connected**.
6. Click **OK**.
7. Login to SSH and switch user to the root user (`su -`)
8. Execute `mount /dev/cdrom /mnt/cdrom`.
9. Execute `mkdir /var/vmtools`.
10. Execute `chmod 700 /var/vmtools`.
11. Execute `cd /var/vmtools`.
12. Execute `tar zxf /mnt/cdrom/VMwareTools-xx.xx.xx-xxxxxxx.tar.gz`.
13. Execute `umount /mnt/cdrom`.
14. Execute `cd vmware-tools-distrib`.
15. Execute `./vmware-install.pl`.
16. Follow the VWware-Tools installation prompts using all of the default values.
17. After the VMware-Tools has installed successfully, execute `reboot` to restart the server.

## Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

# Adding a virtual hard disk for recording

### Before you begin

Ensure that the vAAC Medium Simplex OVA, Medium Redundant Primary OVA, or Medium Redundant Secondary OVA has been deployed

If the deployed vAAC VM has been powered on, power off the VM.

### About this task

This task adds a virtual hard disk for recording feature. Each vAAC OVA comes with 1.5G of disk space for recording feature. This configuration needs to be reset to the proper size to accommodate the recording feature in production. In this document, it adds 100 virtual hard disk as example.

### Procedure

1. **(Optional)** If the deployed vAAC VM has been powered on, power off the VM:

   In vSphere Client, right click on the vAAC VM and select **Power** > **Power Off**.
2. Right click on the VM and select **Edit Settings...**.
3. In the Edit Settings dialog, click on **Add...**.
4. In the Add Hardware Window, click on **Hard Disk**, and click on **Next**. Select **Create a new virtual disk** and click on **Next**. Configure the following sections:
   a. In the Capacity section, set **Disk Size** to **100 GB**.
   b. In the Disk Provisioning section, select **Thick Provision Lazy Zeroed**.
   c. In Location, select **Specify a datastore or datastore cluster** and click on **Browse…**. Select a proper datastore which has sufficient disk space and click on **Next**.
   d. In Advanced Options, keep all the default selections. Click on **Next**.
   e. View the summary and click on **Finish**. Click on **OK** in the Edit Settings window
5. In vSphere Client, right click on the vAAC VM and select **Power** > **Power On**.
6. After the vAAC fully starts up, login to the VM Element Manager Console and navigate to **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers** > **MediaServer1 (or MediaServer2 if it is a redundant system)** > **NE Maintenance**. Select the Avaya Media Server network element and stop the network element.
7. After the vAAC fully starts up, login to the VM Element Manager Console and navigate to **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Servers and Clusters** > **WCS1 (or WCS2 if it is a redundant system)** > **NE Maintenance**. Select the WCS network element and stop the network element.
8. SSH login to the vAAC system as a `ntsysadm` user and switch to the `root` user by executing the `su -` command.
9. Execute the command `mcpDataDiskMgt.pl -f`, follow the instructions and enter `Y` at the `All information that is currently on it will be lost!  (Y/N) [N]?` prompt.

10. Execute the command `mcpDataDiskMgt.pl -u`.

    At this step, the data disk unmounts successfully from `/var/mcp/data`.

    If the data disk does not unmount successfully, a warning is displayed. If it does not unmount, you should check the disk and unmount it.

11. Execute the command `mcpDataDiskMgt.pl -c`, follow the instruction and enter `Y` at the `All information that is currently on it may be lost!  (Y/N) [N]?` prompt.

12. Execute the command `mcpDataDiskMgt.pl -m`.

    At this step, the data disk unmounts successfully from `/var/mcp/data`.

13. Login to the vAAC Element Manager Console and navigate to **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers** > **MediaServer1 (MediaServer2 if it is a redundant system)**.

14. Click on NE Maintenance and select the Avaya Media Server network element and **Start** the network element.

15. Login to the vAAC Element Manager Console and navigate to **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Servers and Clusters** > **WCS1 (WCS2 if it is a redundant system)**.

16. Click on NE Maintenance and select the WCS network element and **Start** the network element.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

## Deciding the next steps

If yours is an SMB or medium deployment, regardless of whether it provides redundancy, it is likely that you will not have to perform any further installation tasks. For Avaya Aura® Conferencing, Avaya has packaged each of the required network elements within the Avaya Aura® Conferencing software bundle which you have just installed.

**Note:**

*Required network elements* in this context refers to the various components that make up the Avaya Aura® Conferencing system. These network elements include the Web Conferencing Server, which provides document sharing capabilities, the Provisioning Manager, which provides user management functionality, and the Element Manager, which provides device management functionality.

At this point, it is likely that you only need to perform some provisioning tasks. Once you have completed these provisioning tasks, you can verify the end to end functionality of your Avaya Aura® Conferencing system by placing a test call from your configured endpoint. The required provisioning tasks are listed here. You perform each of these tasks using the Provisioning Client application:

- Obtain licenses for Avaya Aura® Conferencing from the Avaya Product Licensing and Delivery System (PLDS).

  If you have installed an Avaya Aura® solution, see Licensing for Avaya Aura deployments on page 171. If you have installed a Turnkey solution, see Licensing for Turnkey deployments on page 163.
- Add the location of your Avaya Aura® Conferencing system.

  If you have installed an Avaya Aura® solution, see Adding a location on page 318. If you have installed a Turnkey solution, see Configuring the PBX location information and dialing rules on page 223.
- Configure the routing policy which applies to your Avaya Aura® Conferencing system.

  If you have installed an Avaya Aura® solution, see Configuring the route to Avaya Aura Conferencing on System Manager on page 309 and Adding MeetMe Adhoc and Event service URIs in Provisioning Client on page 313. If you have installed a Turnkey solution, see Configuring the PBX IP address on page 220.
- Add the communication addresses for your Avaya Aura® Conferencing system.

  If you have installed an Avaya Aura® solution, see Making Avaya Aura Conferencing aware of System Manager domains on page 320 and Adding System Manager domains in Provisioning Client on page 321. If you have installed a Turnkey solution, see Adding a user for Avaya Aura® Conferencing (AAC) for Turnkey on page 228.
- Add some end users.

  As with the other tasks, the process of adding end users depends on your deployment type. If you have installed a Turnkey solution, you can use the Provisioning Client application. If you have installed an Avaya Aura® solution, you can use the Provisioning Client or, ideally, System Manager. Lightweight Directory Access Control (LDAP) integration is available for both types of solution. For more information, see Adding a user from Provisioning Client on page 229 or Assigning the conferencing profile to new System Manager users on page 322.

If your deployment requires the integrated audio and video feature of Avaya Aura® Conferencing, you will have to configure a Flash Media Gateway (FMG). If your deployment is a large deployment, you will also have to perform additional configuration tasks.

However, for many deployments, you can skip much of the remaining content in this manual. Avaya recommends retaining the manual for reference in the future. The manual is essential if you have very advanced configuration requirements or a highly complex deployment environment.

# Chapter 10: Installing Avaya Aura® Conferencing (AAC) for Turnkey using VMWare

## Avaya Aura® Conferencing Turnkey solution overview

The Avaya Aura® Conferencing Turnkey solution is a meet me conferencing solution which provides audio, video, and Web conferencing. The Avaya Aura® Conferencing Turnkey solution provides the ability to deploy Avaya Aura® Conferencing without the Avaya Aura® stack. The Avaya Aura® PBX stack refers to staging and management software such as System Platform and System Manager. With the Avaya Aura® Conferencing Turnkey solution, Avaya Aura® Conferencing can be deployed with a Private Branch eXchange (PBX) such as Avaya Aura® Communication Manager and Avaya Communication Server 1000 with a SIP trunk between Avaya Aura® Conferencing and the PBX.

Users can connect to the conference using audio and/or video by way of any of the PBX clients, by way of Audio Video in Collaboration Agent embedded in Collaboration Agent, or by way of the Avaya Aura® Conferencing mobile clients. Additionally, users can join Web collaboration using the Collaboration Agent interface.

Administrators can manage the Avaya Aura® Conferencing components and users using the Element Manager and Provisioning interfaces. In addition, administrators can bulk provision users by way of Lightweight Directory Access Protocol (LDAP).

Administrators can deploy the Avaya Aura® Conferencing Turnkey solution on bare metal servers. A bare metal environment refers to the installation of a server directly on to hardware rather than within the host operating system. Alternatively, the Avaya Aura® Conferencing Turnkey solution supports virtualization through VMWare.

This solution is available for all deployment models and so is suited to small to medium (SMB), medium, and large enterprises.

The installation, upgrade, and patching of the Avaya Aura® Conferencing Turnkey solution is almost the same as the process of installing, upgrading, and patching the Avaya Aura® Conferencing for Avaya Aura® solution. Moreover, the Avaya Aura® Conferencing user interfaces are identical. End users will be unaware of whether their conference bridge is powered by Avaya Aura® or an alternative PBX.

**Note:**

Avaya Aura® Conferencing is a conferencing feature server. It is not a registrar or a proxy and does not provide proxy functions.

## Support for cascading

Media cascading reduces the number of media streams travelling across the WAN by consolidating these streams based by location. This technique is applied to both audio and video streams. Media cascading provides bandwidth optimization with no significant reductions in the quality of audio or video. Conferences are scalable with proper configuration and management which is fully transparent to end users. Media cascading is available for event conferences. The combination of these two features — event conferencing and media cascading — provides a very compelling solution for very large global conferences.

If the media cascading location and the location of the hosting media server are different, bandwidth is allocated for the audio media stream to allow for participants joining the conference from other locations without blocking. Network bandwidth is used to transmit/receive audio media streams to/from the Hosting Media Server location, although silence suppression significantly reduces the actual bandwidth received from the hosting location. Video bandwidth for media cascading is only allocated and consumed when it is required in the conference. When all of the participants have joined from a single cascading location, video bandwidth between the Cascading Media Server and the Hosting Media Server is only allocated and consumed if a participant from another location joins the conference.

## Cascading capacity

The following table shows the supported capacity for cascading Avaya Aura® Media Servers for Avaya Aura® Conferencing.

| | Capacity (Audio Sessions) | Capacity (Video Sessions ) | CPUs | Memory (GB) | Storage (GB) | CPU Speed (GHZ) | CPU Reservation (GHZ) |
|---|---|---|---|---|---|---|---|
| VMware system:<br>Cascading Avaya Aura® Media Servers (6 vCPUs) | 540 | 160 | 6 | 16 | 150 | 2.893 | 17.358 |
| Bare-metal system:<br>Cascading Avaya Aura® Media Servers | 600 | 180 | 6 | 16 | 150 | 6 (12 with hyperthreading) | N/A |

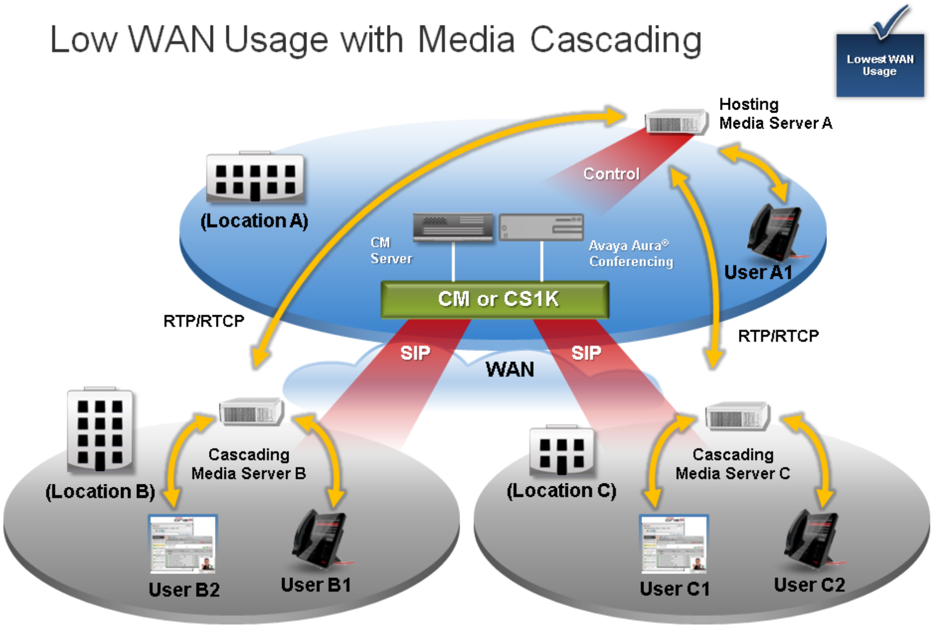


**Figure 20: Network Architecture**

# Introduction to vAAC

Virtualization is becoming more prevalent within enterprise business data centers and is seen as a way to reduce both capital expenditure (capex) and total cost of ownership (TCO). VMware™ is a leader in virtualization technology and seen as an important platform for Avaya to adopt for its enterprise solutions. VMware provides centralized management of virtualized hosts and virtual machines from a single console. It provides a comprehensive suite of tools to help the administrator monitor and manage their data center.

The Avaya Aura® Conferencing on VMware feature creates images with pre-configured and fully functional Avaya Aura® Conferencing software which is packaged in the standard template format (OVA - Open Virtualization Achive) for deploying into the customer's VMware virtual infrastructure. Avaya refers to the virtualized Avaya Aura® Conferencing solution as "vAAC".

In this release, multiple OVAs support the various deployment scenarios:

- vAAC Medium Simplex OVA: AAC RHEL platform + Pre-installed/deployed/configured application bundle (EM, DB, PROV, WCMS, WCS, AS, AMS, AM, DCS, FMG)
  - All NEs are deployed & started automatically.
- vAAC Medium Redundant Primary OVA: AAC RHEL platform + Pre-installed/deployed/configured Medium Primary application bundle (EM, DB, PROV, WCMS, WCS, AS, AMS, AM, DCS, FMG)
  - All NEs (on Primary instances) are deployed & started automatically.

- vAAC Medium Redundant Secondary OVA: AAC RHEL platform + Pre-installed/deployed/configured medium secondary application bundle (EM, DB, PROV, WCMS, WCS, AS, AMS, AM, DCS, FMG)
    - All NEs are deployed & started automatically.
- vAAC Platform: AAC RHEL platform + Application Bundle ISO file.
    - Avaya Aura® Conferencing platform is installed and started.
    - Admin has to run “mcpInstaller” to install AAC NEs.
    - During the vAAC Platform OVA deployment, you, as the customer, can select large platform resources or small platform resources.

✱ **Note:**

VMware is only supported on medium and large deployments and is not supported on SMB deployments.

✱ **Note:**

Use of vMotion for automatic disaster recovery (ADR) is not supported. Instead, you must use the ADR feature of Avaya Aura® Conferencing.

### Flexible deployment: Large platform resources or small platform resources

For this release, Avaya created two platform OVAs (vAAC_LargePlatform and vAAC_SmallPlatform):

- vAAC_LargePlatform OVA‘s vCPU and memory resources: 12 vCPUs (100% reserved), 30 GB Memory (100% reserved)
- vAAC_SmallPlatform OVA’s vCPU and memory resources: 6 vCPUs (100% reserved), 16 GB Memory (100% reserved)

With the exception of the OVA vCPU and memory resource configuration and reservation, all other parameters were the same for these OVAs. These two OVAs were two different entities, which the customer had to download.

For this release, Avaya simplified the two platform OVAs by introducing a flexible deployment feature. Now, there is a single platform OVA. During the platform OVA deployment, the wizard prompts customers to select the deployment configuration. There are two deployment configuration options:

- Large Platform Resources
- Small Platform Resources

With this feature, customers can choose difference resource configuration during the OVA deployment. The Large Platform Resources option is compatible with the Large Platform OVA deployment from previous releases. The Small Platform Resources option is compatible with the Small Platform OVA deployment from previous releases.

The Avaya Aura® Conferencing software will now be supported in VMWare environments that utilize the ESXi 5.1, ESXi 5.5, and ESXi 6 hypervisors. Avaya will provide virtual machine templates called OVA files. These files specify the required number of virtual CPUs, memory, disk space, and disk performance required by the VM. .

## OVA deployment model summary

The following table shows the number of OVAs that are required to deploy each of the deployment models. These are the minimum number of virtual machines (VMs) that are required as per the staging files.

**Note:**

A solution may add additional VMs (using the vAAC Platform OVA) as required, supporting additional optional components.

| OVAs required per deployment | vAAC-Medium Simplex OVA | vAAC-Medium Redundant Primary OVA | vAAC-Medium Redundant Secondary OVA | vAAC-Platform OVA<br>(with Large Platform Resources Deployment Option) | vAAC-Platform OVA<br>(with Small Platform Resources Deployment Option) |
|---|---|---|---|---|---|
| Medium Simplex | 1 | | | | 0 to 10 (cascading Avaya Aura® Media Server (MS)s) |
| Medium Redundant | | 1 | 1 | | 0 to 10 (cascading Avaya Aura® Media Server (MS)s) |
| Large Simplex (starting configuration) | | | | 3 | 0 to 32 (cascading Avaya Aura® Media Server (MS)s) |
| Large Redundant (starting configuration) | | | | 6 | 0 to 32 (cascading Avaya Aura® Media Server (MS)s) |
| Large Redundant (expansion) | | | | 8 | 2 Document Conversion Servers (DCS)<br>0 to 32 Avaya Aura® Media Server (MS)s |

**Note:**

Currently, Avaya Aura® Conferencing does not support VMware for the SMB-sized solution. You can only using VMware for medium or large deployments.

## OVA resource reservation requirements

| AAC OVA | Processor<br>vCPUs | Processor<br>Reservation<br>(MHz) | Memory<br>(GB) | Memory reservation (GB) | Disk size<br>(GB) | Physical cores<br>Minimum frequency |
|---|---|---|---|---|---|---|
| Medium Simplex OVA | 8 | 23,144 | 24 | 24 | 150 | 2,893 |
| Medium Redundant Primary OVA | 8 | 23,144 | 24 | 24 | 150 | 2,893 |
| Medium Redundant Secondary OVA | 8 | 23,144 | 24 | 24 | 150 | 2,893 |
| Platform Large Footprint OVA | 12 | 34,716 | 30 | 30 | 150 | 2,893 |
| Platform Small Footprint OVA | 6 | 17,358 | 16 | 16 | 150 | 2,893 |

**Note:**

For medium systems, eight vCPU and 24 GB memory will only support 2000 user capacity. To support 5000 user capacity, you must increase resources to 12 vCPU, 30 GB. You must use the following procedure to update the resource reservation. For more information, see Modifying vAAC OVA resource reservation and the number of CPUs on page 193.

## Cascading capacity

The following table shows the supported capacity for cascading Avaya Aura® Media Servers for Avaya Aura® Conferencing.

| | Capacity (Audio Sessions) | Capacity (Video Sessions ) | CPUs | Memory (GB) | Storage (GB) | CPU Speed (GHZ) | CPU Reservation (GHZ) |
|---|---|---|---|---|---|---|---|
| VMware system:<br>Cascading Avaya Aura® Media Servers (6 vCPUs) | 540 | 160 | 6 | 16 | 150 | 2.893 | 17.358 |
| Bare-metal system: | 600 | 180 | 6 | 16 | 150 | 6 (12 with hyperthreading) | N/A |

*Table continues…*

| | Capacity (Audio Sessions) | Capacity (Video Sessions ) | CPUs | Memory (GB) | Storage (GB) | CPU Speed (GHZ) | CPU Reservation (GHZ) |
|---|---|---|---|---|---|---|---|
| Cascading Avaya Aura® Media Servers | | | | | | | |

**Related links**

Modifying the vAAC OVA resource reservation and the number of CPUs on page 193

## Checklist for installing the AAC Turnkey solution

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Ensure that you are qualified to perform this task. | Ensure that you have the skills required to install, configure, and upgrade Avaya Aura® Conferencing. For a list of the required core competencies, see Audience on page 26. Before undertaking any advanced procedures, you must complete the required Avaya Aura® Conferencing training, as listed in Training on page 23. Avaya recommends that you download all available Avaya Aura® Conferencing documentation, as listed in Documentation on page 20. | | |
| 2 | Read the prerequisites | Prerequisities to running vAAC OVAs on page 178 | | |
| 3 | Deploy the OVAs | Deploying vAAC OVAs on page 179 | | |
| 4 | Configure for your specific deployment type | • If you have a medium deployment without redundancy, see Configuring a vAAC medium simplex system | | |

*Table continues…*

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| | | after the OVA deployment on page 209<br>• If you have a medium deployment with redundancy, see Configuring a vAAC medium redundant primary core server after the OVA deployment on page 212 and Configuring a vAAC medium redundant core server after the OVA deployment on page 215<br>• If you have a large deployment with redundancy, see Installing the components for Avaya Aura® Conferencing for Turnkey on page 141. | | |
| 5 | Perform a number of provisioning tasks to enable you to place a test call to verify the installation. | Read the following section for guidance: Deciding the next steps on page 196 | | |

## Prerequisites to running vAAC OVAs

- You must install ESXi hypervisor. ESXi hypervisor is required on physical hosts for virtualizing resources such as, CPUs, RAMs, NICs and storage. On the ESXi hypervisor, you must ensure that **Hyperthreading** is set to **Active**.
  - vSphere client is the administrative tool for managing ESXi hosts.
  - vCenter server is the management server, through which ESXi resources pools, and other VMware advanced features can be managed or enabled by vSphere client.
  - vMotion is a component of vSphere that allows the live migration of a running virtual machine's (VM) file system from one storage system to another. If you are using vMotion, you must take the network element out of service first. Use of vMotion for automatic disaster recovery (ADR) is not supported. Instead, you must use the ADR feature of Avaya Aura® Conferencing.
- You can create virtual machines on shared storage — in other words, iSCSI NAS (Network Attached Storage), or local attached storage.

**Note:**

The virtual machines have no knowledge of the underlying physical disks. All virtual disks will appear to be SCSI disk drive to virtual machines.

## Deploying vAAC OVAs

Each of the following procedures use VMware vSphere PC client and connects to VMware vCenter. The current procedure applies to all vAAC OVA deployment models.

### Before you begin

Download all required vAAC OVA files to your computer before you begin.

### About this task

Use this task to deploy vAAC OVAs to the VMware Virtual Machine (VM).

### Procedure

1. Login to the vCenter through vSphere PC client.
2. Select a target EXSi host from **vSphere Client** > **Hosts and Clusters view**.
3. Click **File** > **Deploy OVF Template...**.

   The **Deploy OVF Template** wizard begins.
4. At the **Source** step, select the vAAC OVA file from your computer and click **Next**.
5. At the **OVF Template Details** step, display the select OVA file information and click **Next**
6. At the **End User License Agreement** step, read the license agreement, click **Accept** and click **Next**.
7. At the **Name and Location** step, enter a proper VM name and select a proper data center in the **Inventory Location** and click **Next**.
8. At the **Deployment Configuration** step, select the **Large Platform Resources** or the **Small Platform Resources** option and click **Next**

   **Note:**

   If you are deploying the non-platform OVAs, you can skip this step.
9. At the **Storage** step, select the proper storage to which you want to deploy the OVA and click on **Next**.
10. At the **Disk Format** step, select **Thick Provision Lazy Zeroed** and click **Next**.
11. At the **Ready to Complete** step, verify the information and click **Finish**.

    The **VM deployment progress** dialog is displayed
12. After the VM is successfully deployed, select the VM, right click on it, and select **Power** > **Power On**.

### Result

The selected vAAC OVA has been deployed and powered on.

### Next steps

Proceed to Configuring the vAAC platform after the OVA deployment on page 180.

## Configuring the vAAC platform after the OVA deployment

The attribute selections in this procedure reflect a particular example configuration. Your configuration may differ and as such, may require different attribute selections.

### Before you begin

Enter the IP addresses and Fully Qualified Domain Names (FQDN) of each of the server resources in the following table. You will require this information during the configuration.

| Resource Name | IP Address | FQDN |
|---|---|---|
| Primary Element Manager Server | | |
| Element Manager Service | | |
| Accounting Manager Service | | |
| Application Server Service | | |
| Primary Media Server Media Address | | |
| Primary Web Conferencing Server Service | | |
| NTP Server | | |
| DNS Server | | |
| Gateway/Subnet address[7] | | |
| System Manager (SMGR)[7] | | |
| Session Manager (SM) SIP[7] | | |

### About this task

Use this task to configure the vAAC platform after the OVA deployment. This task applies to vAAC Platform Large Platform and Small Platform deployments.

**Tip:**

In order to progress through the VM Console, you can click **Ctrl + Alt + left click**.

### Procedure

1. Right click on the VM and select **Open Console**.

[7] Not required for Turnkey.

2. On the Hostname Configuration screen, type the hostname and press **Enter**.
3. At the confirmation prompt, type `Y` and press **Enter**.

   The Network Configuration screen is displayed.
4. Configure the network, as follows:
   1. At the **Enter IP address** prompt, type the *Primary EM Server IP Address* from the table above.
   2. At the **Enter subnet prefix length (1–38)** prompt, type the appropriate alphanumeric length.
   3. At the **Enter gateway IP address** prompt, type the *Gateway address* from the table above.
   4. At the confirmation prompt, type **Y** and press **Enter**.

      The DNS Configuration screen is displayed.
5. Configure the DNS, as follows:
   1. At the **Domain Suffix(es): Enter Selection** prompt, accept the default configuration by typing `C`.
   2. At the **How many DNS Servers would you like to reference (1–3)** prompt, type the appropriate number, such as `1`.
   3. At the **Enter Primary DNS Server (<DNS server IP address>)** prompt, type the DNS IP address.
   4. At the confirmation prompt, type `Y` and press **Enter**.

      The Configuration Confirmation screen is displayed.
   5. Type `Y` and press **Enter**.

      The Configuration Confirmation screen for the timezone is displayed.
6. Configure the timezone, as follows:
   1. At the **Use the default value (US/Eastern) for this timezone** prompt, type **Y** to use default value or type **N** to reconfigure the timezone.
   2. At the confirmation prompt, type `Y` and press **Enter**.

      The Date and Time screen is displayed.
7. Configure the date and time as follows:
   1. At the **Do you want to keep this date and time (Y/N) [Y]?** prompt, type **Y** to use current date and time or type **N** to reconfigure the date and time.
   2. At the confirmation prompt, type **Y** and press **Enter**.

   The NTP Configuration screen is displayed.
8. Configure the NTP server. For more information, see Configuring the NTP clock on page 127.

9. Configure the SysLog server details, as follows:

    a. At the **Do you wish to configure/unconfigure/display the SysLog Server IP Address?** prompt, type `u`.

    b. At the confirmation prompt, type `Y` and press **Enter**.

    The Encrypt Recording Data Disk screen is displayed.

10. Configure encryption of the recording data disk, as follows:

    a. At the **Do you wish to encrypt the recording data disk? (Y/N) [N]?** prompt, type **N** to use the default non-encryption for the recording data disk, then press **Enter** to continue. Alternatively, you can type **Y** to configure the recording data disk encryption.

    b. To configure encryption, type Y and enter a phrase in the **Enter the encryption secure phrase** and **Enter the encryption secure phrase again** fields.

    c. At the confirmation prompt, type `Y` and press **Enter**.

11. Press **Enter** to finish.

### Result

The vAAC platform is configured.

### Next steps

It is a good idea to back up the platform at this point.

⚠ **Warning:**

> After the installation, you need to provide a platform back-up. If you do not back up the platform then during the platform failure, all information on the recording data disk is lost. There is no other way to restore or recreate the encrypted secure phrase.

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

## Configuring a vAAC medium simplex system after the OVA deployment

The steps in this section apply to a Turnkey deployment. If yours is an Avaya Aura® deployment, see Configuring a vAAC medium simplex system after the OVA deployment on page 182.

### Before you begin

- Enter the IP addresses and Fully Qualified Domain Names (FQDN) of each of the server resources in the following table. You will require this information during the configuration.

| Resource Name | IP Address | FQDN |
|---|---|---|
| Primary Element Manager Server | | |
| Element Manager Service | | |
| Accounting Manager Service | | |
| Application Server Service | | |
| Primary Media Server Media address | | |
| Primary Web Conferencing Server Service | | |
| Primary Provisioning Manager | Same as Primary Element Manager Server IP | |
| Primary Web Collaboration Agent Manager | Same as Primary Element Manager Server IP | |
| Primary Document Conversion Server | Same as Primary Element Manager Server IP | |
| FMG (Flash Media Gateway) Server | | |
| NTP Server | | |
| DNS Server | | |

- Complete the steps in Configuring the vAAC platform after the OVA deployment on page 180.

## About this task

Use this task to configure a vAAC medium simplex deployment.

**Tip:**

In order to progress through the VM Console, you can click **Ctrl + Alt + left click**.

## Procedure

1. If this is the Turnkey configuration, please select option 2: AAC connected to a SIP base PBX (CM, CS1K, IPO, etc) on the Avaya Aura® Conferencing System Deployment Type Configuration screen.
2. On the Avaya Aura® Conferencing Core Application Configuration screen, configure the core application IP addresses, as follows:
    a. At the **Please enter the Service IPv4 address of Element Manager** prompt, enter the *EM Service IP* address from the table above.
    b. At the **Please enter the Service IPv4 address of Accounting Manager** prompt, enter the *Accounting Manager Service IP* from the table above.
    c. At the **Please enter the Service IPv4 address of Application Server** prompt, enter the *Application Server IP* from the table above.
    d. At the **Please enter the Media IPv4 address of the primary media server** prompt, enter the *Primary Media Server IP* from the table above.

e. At the **Please enter the Service IPv4 address of the primary Web Conferencing Server** prompt, enter the *Primary WCS Service IP* from the table above.

f. At the **Please enter the FQDN for the Service address of the Element Manager** prompt, enter the Service address of the Element Manager FQDN from the table above.

g. At the **Please enter the FQDN for the primary Provisioning Manager** prompt, enter the primary *Provisioning Manager FQDN* from the table above.

h. At the **Please enter the FQDN for the primary Web Conferencing Server** prompt, enter the primary *Web Conferencing Server FQDN* from the table above.

i. At the **Please enter the FQDN for the primary Collaboration Agent Manager** prompt, enter the *primary Collaboration Agent Manager FQDN* from the table above.

j. At the **Please enter the FQDN for the primary Document Conversion Server** prompt, enter the primary *Document Conversion Server FQDN* from the table above.

k. At the **Please enter the Site Name of this AAC installation** prompt, enter a short name for the site you are configuring.

l. At the **Please enter the Site Long Name of this AAC installation** prompt, enter a longer name for the site you are configuring.

3. On the Flash Media Gateway (FMG) Configuration screen, configure the FMG as follows:

a. At the **Enter the IP address for JMX Connections** prompt, type the *FMG Server IP address* from the table above.

b. At the **Enter the IP address for RTMP Connections** prompt, type the *FMG Server IP address* from the table above.

c. At the **Enter the IP address for HTTP Connections** prompt, type the *FMG Server IP address* from the table above.

d. At the **Enable RTMPS?** prompt, type `yes`.

e. At the **Enter the Port for RTMPS** prompt, enter the port number for RTMPS connections.

f. At the **Generate a self-signed certificate for RTMPS (Port 443)** prompt, type `yes`.

g. At the **Enable RTMP?** prompt, type `yes`.

h. At the **Enter the Port for RTMP** prompt, type `1935`.

i. At the **Enable RTMPT?** prompt, type `yes`.

j. At the **Enter the Port for RTMPT** prompt, type `80`.

k. In the **Management Configuration** section, at the **Enter the IP address for Management Client** prompt, type the *FMG Server IP address* from the table above.

l. At the **Enter the Port for Management Client** prompt, enter the port number for management client connections.

m. At the **Generate a self-signed certificate for RTMPS for Management Portal** prompt, type `yes`.

The FMG is configured.

## Configuring a vAAC medium redundant primary core server after the OVA deployment

### Before you begin

- Enter the IP addresses and Fully Qualified Domain Names (FQDN) of each of the server resources in the following table. You will require this information during the configuration.

| Resource Name | IP Address | FQDN |
|---|---|---|
| Primary Element Manager Server | | |
| Secondary Element Manager Server | | |
| Element Manager Service | | |
| Accounting Manager Service | | |
| Application Server Service | | |
| Primary Media Server Media address | | |
| Secondary Media Server Media address | | |
| Primary Web Conferencing Server (WCS) Service | | |
| Primary Provisioning Manager | Same as Primary Element Manager Server IP | |
| Secondary Provisioning Manager | Same as Secondary Element Manager Server IP | |
| Primary Web Collaboration Agent Manager | Same as Primary Element Manager Server IP | |
| Secondary Web Collaboration Agent Manager | Same as Secondary Element Manager Server IP | |
| Primary Document Conversion Server | Same as Primary Element Manager Server IP | |
| Secondary Document Conversion Server | Same as Secondary Element Manager Server IP | |
| Secondary Web Conferencing Server (WCS) Service | | |
| FMG Server IP on Primary | | |
| NTP Server | | |
| DNS Server | | |

- Complete the steps in Configuring the vAAC platform after the OVA deployment on page 180.

## About this task

Use this task to configure a vAAC medium redundant primary core server.

## Procedure

1. If this is the Turnkey configuration, please select option 2: AAC connected to a SIP base PBX (CM, CS1K, IPO, etc) on the Avaya Aura® Conferencing System Deployment Type Configuration screen.
2. On the Avaya Aura® Conferencing Core Application Configuration screen, configure the core application IP addresses, as follows:
    a. At the **Please enter the Internal OAM (Default) IPv4 address of the secondary Element Manager server** prompt, enter the *Secondary Element Manager Server* address from the table above.

    b. At the **Please enter the Service IPv4 address of Element Manager** prompt, enter the *EM Service IP* address from the table above.

    c. At the **Please enter the Service IPv4 address of Accounting Manager** prompt, enter the *Accounting Manager Service IP* from the table above.

    d. At the **Please enter the Service IPv4 address of Application Server** prompt, enter the *Application Server IP* from the table above.

    e. At the **Please enter the Media IPv4 address of the primary media server** prompt, enter the *Primary Media Server IP* from the table above.

    f. At the **Please enter the Media IPv4 address of the secondary media server** prompt, enter the *Secondary Media Server IP* from the table above.

    g. At the **Please enter the Service IPv4 address of the primary Web Conferencing Server** prompt, enter the *Primary WCS Service IP* from the table above.

    h. At the **Please enter the Service IPv4 address of the secondary Web Conferencing Server** prompt, enter the *Secondary WCS Service IP* from the table above.

    i. At the **Please enter the FQDN for the Service address of the Element Manager** prompt, enter the *Service address of the Element Manager FQDN* from the table above.

    j. At the **Please enter the FQDN for the primary Provisioning Manager** prompt, enter the *Primary Provisioning Manager FQDN* from the table above.

    k. At the **Please enter the FQDN for the secondary Provisioning Manager** prompt, enter the *Secondary Provisioning Manager FQDN* from the table above.

    l. At the **Please enter the FQDN for the primary Web Conferencing Server** prompt, enter the *Primary Web Conferencing Server FQDN* from the table above.

    m. At the **Please enter the FQDN for the secondary Web Conferencing Server** prompt, enter the *Secondary Web Conferencing Server FQDN* from the table above.

n. At the **Please enter the FQDN for the primary Collaboration Agent Manager** prompt, enter the *Primary Collaboration Agent Manager FQDN* from the table above.

o. At the **Please enter the FQDN for the secondary Collaboration Agent Manager** prompt, enter the *Secondary Collaboration Agent Manager FQDN* from the table above.

p. At the **Please enter the FQDN for the primary Document Conversion Server** prompt, enter the *Primary Document Conversion Server FQDN* from the table above.

q. At the **Please enter the FQDN for the secondary Document Conversion Server** prompt, enter the *Secondary Document Conversion Server FQDN* from the table above.

r. At the **Please enter the Site Name of this AAC installation** prompt, enter a short name for the site you are configuring.

s. At the **Please enter the Site Long Name of this AAC installation** prompt, enter a longer name for the site you are configuring.

t. Press **Enter** to continue.

3. On the Flash Media Gateway (FMG) Configuration screen, configure the FMG as follows:

a. At the **Enter the IP address for JMX Connections** prompt, type the *FMG Server IP address* from the table above.

b. At the **Enter the IP address for RTMP Connections** prompt, type the *FMG Server IP address* from the table above.

c. At the **Enter the IP address for HTTP Connections** prompt, type the *FMG Server IP address* from the table above.

d. At the **Enable RTMPS?** prompt, type `yes`.

e. At the **Enter the Port for RTMPS** prompt, enter the port number for RTMPS connections.

f. At the **Generate a self-signed certificate for RTMPS (Port 443)** prompt, type `yes`.

g. At the **Enable RTMP?** prompt, type `yes`.

h. At the **Enter the Port for RTMP** prompt, type `1935`.

i. At the **Enable RTMPT?** prompt, type `yes`.

j. At the **Enter the Port for RTMPT** prompt, type `80`.

k. In the **Management Configuration** section, at the **Enter the IP address for Management Client** prompt, type the *FMG Server IP address* from the table above.

l. At the **Enter the Port for Management Client** prompt, enter the port number for management client connections.

m. At the **Generate a self-signed certificate for RTMPS for Management Portal** prompt, type `yes`.

The FMG is configured.

### Result

The FMG is configured.

The vAAC progresses through an initial configuration phase.

The vAAC installs certificates and displays a progress counter. When the configuration is complete, all primary network elements are up and running.

### Next steps

Proceed to Configuring a vAAC medium redundant secondary core server after the OVA deployment on page 215.

## Configuring a vAAC medium redundant secondary core server after the OVA deployment

The table of IP addresses and FQDNs that you use in this task should contain the same information that you used in Configuring a vAAC medium redundant primary core server after the OVA deployment on page 212.

### Before you begin

- Enter the IP addresses and Fully Qualified Domain Names (FQDN) of each of the server resources in the following table. You will require this information during the configuration.

| Resource Name | IP Address | FQDN |
|---|---|---|
| Primary Element Manager Server | | |
| Secondary Element Manager Server | | |
| Element Manager Service | | |
| Accounting Manager Service | | |
| Application Server Service | | |
| Primary Media Server Media address | | |
| Secondary Media Server Media address | | |
| Primary Web Conferencing Server (WCS) Service | | |
| Primary Provisioning Manager | Same as Primary Element Manager Server IP | |
| Secondary Provisioning Manager | Same as Secondary Element Manager Server IP | |

*Table continues…*

| Resource Name | IP Address | FQDN |
|---|---|---|
| Primary Web Collaboration Agent Manager | Same as Primary Element Manager Server IP | |
| Secondary Web Collaboration Agent Manager | Same as Secondary Element Manager Server IP | |
| Primary Document Conversion Server | Same as Primary Element Manager Server IP | |
| Secondary Document Conversion Server | Same as Secondary Element Manager Server IP | |
| Secondary Web Conferencing Server (WCS) Service | | |
| FMG Server IP on Primary | | |
| NTP Server | | |
| DNS Server | | |

- Complete the steps in Configuring the vAAC platform after the OVA deployment on page 180.

### About this task

Use this task to configure a vAAC medium redundant secondary core server.

### Procedure

1. Configure the Avaya Aura® Conferencing Core Application only for Secondary, as follows:

   At the **Please enter the Internal OAM (Default) IPv4 address of the primary Element Manager server** prompt, enter the Primary EM Server IP address from the table above.

   The vAAC configuration automatically continues and displays a progress counter. When the configuration is complete, all network elements are up and running.

2. On the Flash Media Gateway (FMG) Configuration screen, configure the FMG as follows:

   a. At the **Enter the IP address for JMX Connections** prompt, type the *FMG Server IP address* from the table above.

   b. At the **Enter the IP address for RTMP Connections** prompt, type the *FMG Server IP address* from the table above.

   c. At the **Enter the IP address for HTTP Connections** prompt, type the *FMG Server IP address* from the table above.

   d. At the **Enable RTMPS?** prompt, type `yes`.

   e. At the **Enter the Port for RTMPS** prompt, enter the port number for RTMPS connections.

   f. At the **Generate a self-signed certificate for RTMPS (Port 443)** prompt, type `yes`.

   g. At the **Enable RTMP?** prompt, type `yes`.

   h. At the **Enter the Port for RTMP** prompt, type `1935`.

i. At the **Enable RTMPT?** prompt, type `yes`.

j. At the **Enter the Port for RTMPT** prompt, type `80`.

k. In the **Management Configuration** section, at the **Enter the IP address for Management Client** prompt, type the *FMG Server IP address* from the table above.

l. At the **Enter the Port for Management Client** prompt, enter the port number for management client connections.

m. At the **Generate a self-signed certificate for RTMPS for Management Portal** prompt, type `yes`.

   The FMG is configured.

3. The vAAC progresses through an initial configuration phase. The vAAC displays a progress counter.
4. The results are displayed in the VM Console window.
5. At the **Press ENTER to reboot the vAAC to complete OVA configuration...** prompt, press **Enter** to reboot the vAAC.

## Result

The configuration of the secondary server is complete.

## Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

# Chapter 11: Configuring Avaya Aura® Conferencing (AAC) for Turnkey

## Configuration checklist

For this release, Avaya has tested and verified the Avaya Aura® Conferencing Turnkey solution with a number of Private Branch Exchanges (PBXs). These PBXs include Avaya Aura® Communication Manager (CM), Avaya IP Office, and Avaya Communication Server 1000 (CS1K).

In each case, the steps involved in configuring the Avaya Aura® Conferencing Turnkey solution to operate with these PBXs are similar. You must perform a number of tasks on the PBX side and you must perform a number of tasks on the Avaya Aura® Conferencing side.

To learn more about the configuration tasks on the PBX side, Avaya recommends that you download the relevant guides from https://support.avaya.com/. For example:

- *Communication Server 1000E Installation and Commissioning*
- *Implementing Avaya Aura® Communication Manager*
- *Administering Avaya Aura® Communication Manager*
- *Installing IP Office*

In terms of the Avaya Aura® Conferencing side, the steps involved in configuring the solution to operate with Transmission Control Protocol (TCP) mode are relatively straightforward. You simply add the PBX as a SIP entity on Avaya Aura® Conferencing. However, in order to enable the solution to operate with Transport Layer Security (TLS) mode, you must perform two additional steps on Avaya Aura® Conferencing:

- You must add a certificate for the PBX to the Avaya Aura® Conferencing trust store.
- You must configure the SIP entity to use TLS mode, using Element Manager.

You must also perform the corresponding steps on the PBX side.

The following checklist shows the tasks involved in configuring Avaya Aura® Conferencing for Turnkey. These are general guidelines and the precise details vary depending on your choice of PBX.

**Note:**

It is important to note that if you install your system using the VMWare framework, which uses OVA files, many of these configuration tasks are automated. You will not have to perform them manually. However, if you install your system using a baremetal installation, you must perform the configure steps manually.

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Configure the PBX IP address on Avaya Aura® Conferencing | Configuring the PBX IP address on page 220 | This task includes the configuration of the PBX as a SIP entity on Avaya Aura® Conferencing using the Element Manager Console interface. | |
| 2 | Verify access to the Provisioning Client | Verifying local emergency access to the Provisioning Client on page 299 | | |
| 3 | Add the Avaya Aura® Conferencing SIP domain to the Provisioning Client. | Adding the Avaya Aura® Conferencing (AAC) SIP domain on page 222 | | |
| 4 | Add the Avaya Aura® Conferencing location to the Provisioning Client. | Adding a location on page 318 | | |
| 5 | Configure the PBX location address pattern. | Configuring the PBX location address pattern and dialing rules on page 223 | | |
| 6 | Add a service URI. | Adding service URIs for Turnkey on page 225 | | |
| 7 | Configure the address that appears on the Avaya Aura® Conference Manager Add-in for Microsoft Outlook® notification e-mails. | Configuring a Web conferencing host on page 226 | | |
| 8 | Add a user. | Adding a user for Avaya Aura® Conferencing (AAC) for Turnkey on page 228 | | |
| 9 | Configure the media server. | • Assigning media server clusters to locations on page 319<br>• Assigning media server clusters to a physical location on page 319 | You must perform this task even if your media server “cluster” only has a single media server. That is to say — it is a cluster of one. | |

*Table continues…*

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 10 | Perform the corresponding tasks on the PBX side | For example, use the CS1000 Element Manager to configure Avaya Communication Server 1000 (CS1K) to route to Avaya Aura® Conferencing. | This Avaya Aura® Conferencing documentation does not describe how to configure each of the supported PBXs. You must download the PBX documentation in order to learn more about the configuration of each PBX. | |
| If you want to use TLS mode, you must additionally complete the following tasks. | | | | |
| 11 | Add the PBX security certificate to the Avaya Aura® Conferencing trust store. | Importing CA certificates from a third party certificate authority on page 562 | | |
| 12 | If you have not already done so, ensure that the PBX SIP Entity is configured for TLS | Configuring the PBX SIP Entity for TLS on page 226 | | |
| 13 | Perform the corresponding tasks on the PBX side | For example:<br>• Add the Avaya Aura® Conferencing security certificate to the PBX trust store.<br>• Create and export a security certificate for the PBX.<br>• Switch the PBX to use TLS instead of TCP. | | |

## Configuring the PBX IP address

These steps are general guidelines only. The precise configuration details depend on the type of PBX. Avaya Aura® Conferencing is configured to operate in a TLS environment by default. As a result, if you want to deploy the solution in a TCP environment, you must perform the optional steps at the end of this task.

**Tip:**

You may wish to configure the solution to operate in a TCP environment when you first install it. Once you verify the installation, you can choose to update the configuration settings to suit a TLS environment.

### Before you begin

On the PBX side, configure the PBX to route to Avaya Aura® Conferencing.

### About this task

Use this procedure to add the IP address, add an external node, and create a SIP entity.

### Procedure

1. In the navigation pane of Element Manager Console, click **Addresses**.
2. In the Addresses window, click **Add (+)**.
3. In the Add IPv4 Address dialog box, complete the following fields:
    - **Logical Name**: Type the logical name for the PBX (for example CS1K).
    - **IPv4 Address**: Type the IP address for the PBX.
4. Click **Apply**.
5. In the navigation pane of Element Manager Console, select **External Nodes**.
6. In the External Nodes window, click **Add (+)**.
7. In the Add External Node dialog box, complete the following fields:
    - **Name**: Type the logical name for the PBX (for example CS1K).
    - **IPv4 Address**: Select the IP address you added in Step 3.
8. Click **Apply**.
9. In the navigation pane of Element Manager Console, select **SIP Entity**.
10. In the SIP Entity window, click **Add (+)**.
11. In the Add SIP Entity dialog box, complete the following fields:
    - **Short Name**: Type the short name of the PBX.
    - **Long Name**: Type the long name of the PBX.
    - **Trusted**: Select this checkbox.
    - **ExemptDosProtection**: Do not select this checkbox.
    - **Perform Monitoring**: Select this checkbox.
    - **SIP Profile**: Leave blank.
    - **Node**: Select the external node that you added in step 7.
    - **Enable TCP Port**: If the PBX is configured for non-secure access, select this check box and enter 5060 in the **SIP TCP Port** field.

- **Enable TLS Port**: If the PBX is configured for secure access, select this check box and enter 5061 in the **SIP TLS Port** field.

If the PBX is configured with a TLS certificate that is signed by a non-System Manager Certificate Authority, you must export a copy of the Certificate Authority certificate and place the certificate in **Security** > **Certificate Management** > **Truststore** in Element Manager Console.

12. Click **Apply**.
13. **(Optional)** If your PBX is configured with TCP, rather than TLS, you must change some default settings on Avaya Aura® Conferencing because when Avaya ships Avaya Aura® Conferencing, it is configured to operate in a TLS environment by default. As a result, you must enable a setting called **Enable SIP TCP Port** on the following network elements: The application server, media server, Collaboration Agent, and Provisioning Manager. You must also enable a setting called **Enable HTTP Port** on the Web Conferencing Management Server (WCMS). To do this:

    a. On the Element Manager console, stop the network element. For more information, see Stopping a network element instance on page 659.

    b. Navigate to the network element. Updating service FQDNs on page 667 shows some examples of how to navigate to the various network element instances.

    c. Select **Enable SIP TCP Port** on the network element properties.

    d. Restart the network element. For more information, see Starting a network element instance on page 669.

    e. Repeat these steps on the application server, media server, Collaboration Agent, and Provisioning Manager.

    f. Navigate to the WCMS.

    g. Select **Enable HTTP Port** on the network element properties. Save and close the dialog.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

## Adding the Avaya Aura® Conferencing SIP domain

One of the first tasks that you must complete is the configuration of the Avaya Aura® Conferencing SIP domain in the Provisioning Client interface.

### About this task

Use this task to add the Avaya Aura® Conferencing SIP domain to the Provisioning Client in a Turnkey solution.

### Procedure

1. In the Provisioning Client window, select **System Management > User Domains**.
2. In the User Domain box, enter the name of the domain you want to add.
3. Click **Add**.

### Next steps

Inform you PBX network administrator of this value. They must configure this setting on the PBX.

## Adding a location

### Before you begin

You must be logged into Provisioning Client.

### About this task

Use this procedure to add a location.

### Procedure

1. In the Provisioning Client window, select **System Management > Routing > Locations**.
2. Click **Add Location**.
3. In the Location Name box, enter the name of the location.

   If your deployment is an Avaya Aura® deployment, this name must match the location name in System Manager.
4. In the Location Description box, enter any pertinent information about the location.
5. Click **Save**.

## Configuring the PBX location address pattern and dialing rules

These steps are general guidelines only. The precise configuration details depend on the type of PBX.

### Before you begin

- You must be logged into Provisioning Client.
- Your login must have Expert mode privileges to perform this procedure.

### About this task

Use this task to add an IP address pattern for the location that you have just added. For example, if your users will be calling from a client whose IP address starts with 10 then you can add the pattern: 10.*

### Procedure

1. In the Provisioning Client window, navigate to **System Management** > **Routing** > **Locations** > **Location Address Pattern**.
2. From the **Select location** drop-down list, select the entry that you just added.
3. In the **IP Address Pattern** field, add an IP address pattern for the location that is to serve to PBX user.

   For example, if your users will be calling from their PCs and their PCs have an IP address beginning with 47, you could add the following pattern: `47.*`
4. **(Optional)** In the **Notes** field, enter a free text note.
5. Click **Save**.
6. If you wish to support outdial in your deployment, you must add the dialing rules that are used by your PBX.

   Outdial, in this context, refers to a feature whereby conference participants can dial out from the Avaya Aura® Conferencing audio line to another line. For example, they may wish to invite another person into the conference. To activate dialout mode, participants can enter ***1** on their telephone keypad. If you do not wish to support this feature in your deployment, you may not have to configure dialing rules. However, your PBX may require certain translation patterns for incoming calls too. Please consult your PBX administrator to learn more about any required dialing rules for your deployment.
7. **(Optional)** If your PBX is the Avaya Communication Server 1000 (CS1K):
   a. In the Provisioning Client window, navigate to **System Management** > **Dialing Rules** > **PreTranslation**.
   b. Add a pre-translation rule for dial-in calls to Avaya Aura® Conferencing from the CS1K.

      When you create a dial-out rule on the **Translation** tab for the CS1K, you must ensure that the **Phone Context** field on the **PreTranslation** tab matches the **Optional Phone Context** field on the **Translation** tab.
   c. Click **Save**.
8. **(Optional)** On the **Translation** tab, add a translation rule for dial-out calls to the PBX from Avaya Aura® Conferencing.
9. Click **Save**.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

# Adding service URIs for Turnkey

Service URI is the dialing access number for participants to join an Avaya Aura® Conferencing MeetMe conference. The Service URI is the user name part of the SIP URI string.

## About this task

Use the following procedure to add a conference URI.

## Procedure

1. In the Provisioning Client window, select **System Management > Routing > Service URI**.
2. On the Service URI tab, complete the following for a MeetMe conference:
    - **Service URI**: Type an access number for a MeetMe conference.
    - **Locale**: Select a location from the list. The locale specifies the default locale of prompts that are used if your SIP client does not provide your locale.
    - **Conference Type**: Select **MeetMe** from the list.
3. Click **Save**.
4. On the Service URI tab, complete the following for an Adhoc conference:
    - **Service URI**: Type an access number for an Adhoc conference.
    - **Locale**: Select a location from the list. The locale specifies the default locale of prompts that are used if your SIP client does not provide your locale.
    - **Conference Type**: Select **Adhoc** from the list.
5. Click **Save**.
6. On the Service URI tab, complete the following for an Event conference:
    - **Service URI**: Type an access number for an Event conference. This number must match the routing pattern that you configured in System Manager.
    - **Locale**: Select a location from the list. The locale specifies the default locale of prompts that are used if your SIP client does not provide your locale.
    - **Conference Type**: Select **Event** from the list.
7. Click **Save**.
8. Repeat Steps 2 through 7 to add additional conference access numbers.

## Next steps

Configure display numbers in Provisioning Client or refer back to your checklist for more information about your next task.

# Configuring a Web conferencing host

This task is particularly significant if you plan to deploy the Avaya Aura® Conference Manager Add-in for Microsoft Outlook®. You will require the Web conferencing host name during the configuration of the Avaya Aura® Conference Manager Add-in for Microsoft Outlook®.

### About this task

Use the following procedure to configure a Web conferencing host name.

### Procedure

1. In the Provisioning Client window, select **System Management** > **Routing** > **Collaboration Agent Service FQDN**.
2. In the FQDN field, enter an FQDN name.

   Depending on the deployment type, you should enter either:

   - The fully qualified domain name (FQDN) of the Provisioning Manager network element/ Collaboration Agent network element.
   - The FQDN of the load balancer.
3. Click **Save**.

**Related links**

Deploying the Avaya Aura Conference Manager Add-in for Microsoft Outlook on page 622
Implementing a ClickOnce deployment on page 623
Implementing a centralized software deployment on page 625

# Configuring the PBX SIP entity for Transport Layer Security (TLS)

These steps are general guidelines only. The precise configuration details depend on the type of PBX.

### About this task

Use this task to ensure that the SIP entity that you have created on Element Manager to represent the PBX is configured to use TLS mode.

### Procedure

1. In the navigation pane of Element Manager Console, select **SIP Entity**.
2. In the SIP Entity window, click **Edit (+-)**.
3. In the Edit SIP Entity dialog box, ensure that the following field is selected:

   - **Enable TLS Port**: If the PBX is configured for secure access, select this check box and enter 5061 in the **SIP TLS Port** field.

4. Click **Apply**.

### Next steps

Proceed to user provisioning. For more information, see Options for user provisioning on page 228.

# Chapter 12: Provisioning users on Avaya Aura® Conferencing (AAC) for Turnkey

## Options for user provisioning

If you are deploying Avaya Aura® Conferencing (AAC) for Turnkey, you have two options for managing your end-users. You can choose to import groups of users using Lightweight Directory Access Protocol (LDAP) or you can choose to add users using the Provisioning Client interface.

### Managing single users

You can use the Provisioning Client for the management of users. For more information, see Adding a user for Avaya Aura® Conferencing (AAC) for Turnkey on page 228.

### Managing bulk users

You can use LDAP for importing large groups of users. For more information, see Integrating AAC with LDAP directory servers on page 498.

## Adding a user for Avaya Aura® Conferencing (AAC) for Turnkey

You can add a new user for Avaya Aura® Conferencing (AAC) for Turnkey using the Provisioning Client. The Provisioning Client contains some tabs relating to System Manager, such as the **Aura user details** tab. You can ignore these tabs if you are deploying Avaya Aura® Conferencing (AAC) for Turnkey in your customer site.

**Related links**

Adding a user from Provisioning Client on page 229
Modifying a user on page 234
Modifying multiple users at one time on page 235
Modifying a user's conferencing settings on page 237
Deleting a user on page 240

# Adding a user from Provisioning Client

## Before you begin

- You must be logged into Provisioning Client.
- Your login must have Expert mode privileges to perform this procedure.

## About this task

Use this procedure to add a user from Provisioning Client.

## Procedure

1. In the Provisioning Client window, select **User Management > Add User**.
2. Complete this page. See Add User page field descriptions on page 230.
3. Click **Save**.
4. Click the **Communication Address** tab.
5. In the Communication Address box, enter the address for this user.
6. From the System Manager (or User) Domain box, select the User domain for this user.
7. Click **Add**.
8. Repeat Steps 5 through 7 to enter other communication addresses for this user (if necessary).
9. Click the **Password** tab, and complete this page. See Password tab field descriptions on page 232.
10. Click the **User details** tab, and complete this page. See Aura user details tab field descriptions on page 233.
11. Click **Save**.
12. Click the **Actions** tab.
13. Click **Conferencing**.
14. Complete the Conferencing User page for this user. See Conferencing User page field descriptions on page 238.
15. Click **Save**.

### Related links

Adding a user for Avaya Aura Conferencing (AAC) for Turnkey on page 228
Add User page field descriptions on page 230
Base data tab field descriptions on page 231
Communication Address tab field descriptions on page 232
Password tab field descriptions on page 232
Associated Phone Numbers tab field descriptions on page 233
User details tab field descriptions on page 233

Actions tab field descriptions on page 233

## Add User page field descriptions

| Name | Description |
|---|---|
| **Type** | Your only option is **Conferencing**. |
| **Login Name** | This is the user's login name on System Manager in an Avaya Aura® deployment.<br>In an Avaya Aura® Turnkey deployment, the values for **Login Name** and **Communication Profile** can be any value, as long as your entries adhere to the field alphanumeric rules. These fields perform no external validation against a PBX. |
| **Communication Profile** | This is the System Manager communication profile for this user in an Avaya Aura® deployment.<br>In an Avaya Aura® Turnkey deployment, the values for **Login Name** and **Communication Profile** can be any value, as long as your entries adhere to the field alphanumeric rules. These fields perform no external validation against a PBX. |
| **Password** | This is the password for the user's account. This password is used for local authentication. |
| **Confirm password** | This is the password for the user's account. |
| **User Template** | This is the Provisioning Client user template that will be assigned to this account. |
| **Status reason** | Specifies the status for this account.<br>Your choices are:<br>• **ACTIVE**<br>• **INACTIVE** |
| **Location** | Specifies the location for this user. This location should match an existing location in System Manager (or your PBX equivalent). |
| **First name** | You can enter alphanumeric characters. |
| **Last name** | You can enter alphanumeric characters. |
| **Enterprise Identity** | This is the identification (ID) of the user. This field is required for lightweight directory access protocol (LDAP) integration. |
| **Enterprise Domain`** | This is the domain of the enterprise directory. This field is required for LDAP integration. |
| **E-mail** | This is the user's email address. |
| **Business phone** | This is the user's business telephone number. |

*Table continues…*

| Name | Description |
|---|---|
| **Home phone** | This is the user's home telephone number. |
| **Cell phone** | This is the user's cell phone number. |
| **Pager** | This is the user's pager number. |
| **Fax** | This is the user's fax number. |
| **Time zone** | This is the time zone where the user is located. |
| **Locale** | This is the user's preferred written or spoken language. |

**Related links**

Adding a user from Provisioning Client on page 229

## Base data tab field descriptions

| Name | Description |
|---|---|
| **Type** | Your only option is **Conferencing**. |
| **Login Name** | This is the user's login name on System Manager in an Avaya Aura® deployment.<br>In an Avaya Aura® Turnkey deployment, the values for **Login Name** and **Communication Profile** can be any value, as long as your entries adhere to the field alphanumeric rules. These fields perform no external validation against a PBX. |
| **Communication Profile** | This is the System Manager communication profile for this user in an Avaya Aura® deployment.<br>In an Avaya Aura® Turnkey deployment, the values for **Login Name** and **Communication Profile** can be any value, as long as your entries adhere to the field alphanumeric rules. These fields perform no external validation against a PBX. |
| **First name** | You can enter alphanumeric characters. |
| **Last name** | You can enter alphanumeric characters. |
| **Enterprise Identity** | This is the identification (ID) of the user. This field is required for lightweight directory access protocol (LDAP) integration. |
| **Enterprise Domain`** | This is the domain of the enterprise directory. This field is required for LDAP integration. |
| **E-mail** | This is the user's email address. |
| **Business phone** | This is the user's business telephone number. |
| **Home phone** | This is the user's home telephone number. |
| **Cell phone** | This is the user's cell phone number. |

*Table continues…*

| Name | Description |
|---|---|
| **Pager** | This is the user's pager number. |
| **Fax** | This is the user's fax number. |
| **Status reason** | Specifies the status for this account.<br>Your choices are:<br>• **ACTIVE**<br>• **INACTIVE** |
| **Time zone** | This is the time zone where the user is located. |
| **Locale** | This is the user's preferred written or spoken language. |
| **Location** | Specifies the location for this user. This location should match an existing location in System Manager (or your PBX equivalent). |

**Related links**

Adding a user from Provisioning Client on page 229

## Communication Address tab field descriptions

| Name | Description |
|---|---|
| **Communication Address** | Specifies the user's communication address. In an Avaya Aura® deployment, this address should be the same as on System Manager. |
| **User Domain** | Specifies the User domain. For a Turnkey solution, this is the SIP domain of the Avaya Aura® Conferencing server that you are using. |
| **Communication Address column** | Displays all of the user's communication addresses. |
| **Launch Collaboration Agent column** | Enables you to log into the user's Collaboration Agent account. |
| **Delete column** | Enables you to delete the associated communication address. |

**Related links**

Adding a user from Provisioning Client on page 229

## Password tab field descriptions

| Name | Description |
|---|---|
| **New password** | This is the password for the user's account. This password is used for local authentication. |
| **Confirm password** | This is the password for the user's account. |

**Related links**

Adding a user from Provisioning Client on page 229

## Associated Phone Numbers tab field descriptions

| Name | Description |
|---|---|
| **Associated Phone Numbers column** | Displays the telephone numbers that are permanently associated with the selected user. A user can have up to 10 associated telephone numbers. |
| **Delete** | Deletes the corresponding phone number that is associated with the selected user.<br>**Note:**<br>You can only view or delete the associated phone numbers. You cannot edit them. |

**Related links**

Adding a user from Provisioning Client on page 229

## User details tab field descriptions

| Name | Description |
|---|---|
| **Login Name** | This is the user's login name on System Manager in an Avaya Aura® deployment. |
| **Localized Display Name** | This is the localized name that is displayed for this user in a conference list. |
| **Endpoint Display Name** | This is the name that is displayed for this user's endpoint in a conference list. |

**Related links**

Adding a user from Provisioning Client on page 229

## Actions tab field descriptions

| Name | Description |
|---|---|
| **Delete User** | Deletes the selected user. |
| **Conferencing** | Displays the user's conferencing settings. |
| **Clear Lockout** | Clears the lock out condition for the user's login. |

**Related links**

Adding a user from Provisioning Client on page 229

# Modifying a user

### Before you begin

- You must be logged into Provisioning Client.
- Your login must have Expert mode privileges to perform this procedure.

**Warning:**

If you have an Avaya Aura® deployment, any changes you make may cause the Provisioning Client data to become out of sync with the data in Avaya Aura System Manager. You should only modify data to fix sync issues that cannot be resolved from the System Manager interface.

### About this task

Use this procedure to modify an existing user.

### Procedure

1. In the Provisioning Client window, select **User Management > Search Users**.
2. From the Search by box, select the user criterion you want to search.
3. In the Search for box, enter the appropriate search information for the user.
4. Click **Search**.
5. In the Login name column, click on the Login Name of the user.
6. On the Base data tab of the User page, make your changes. See Base data tab field descriptions on page 231.
7. Click the **Communication Address** tab, and make your changes. See Communication Address tab field descriptions on page 232.
8. If you want to delete the phone number that is permanently associated with this user, click the **Associated Phone Numbers** tab, and make your changes. See Associated Phone Numbers tab field descriptions on page 233.
9. Click the **Aura user details** tab, and make your changes. See Aura user details tab field descriptions on page 233.
10. Click the **Actions** tab.
11. Click **Conferencing**.
12. On the Conferencing User page, make your changes. See Conferencing User page field descriptions on page 238.
13. Click **Save**.

**Related links**

Adding a user for Avaya Aura Conferencing (AAC) for Turnkey on page 228

# Modifying multiple users at one time

## Before you begin

- You must be logged into Provisioning Client.

⚠ **Warning:**

If you have an Avaya Aura® deployment, any changes you make may cause the Provisioning Client data to become out of sync with the data in Avaya Aura System Manager. You should only modify data to fix sync issues that cannot be resolved from the System Manager interface.

## About this task

Use this procedure to modify the conference class of service, video (enable/disable) setting, and recording (enable/disable) setting for multiple users at one time (that is, bulk provisioning). In this procedure, you will identify the list of users you want to modify by specifying search criteria.

## Procedure

1. In the Provisioning Client window, select **User Management > Bulk Provisioning**.
2. From the Field box, select the user criterion you want to search.
3. From the Operation box, select the search operation you want to perform.
4. In the Value box, specify the appropriate search information for the users.
5. Click **Add Criteria**.

   **Note:**

   You can modify up to 1000 users at any one time.
6. Repeat Steps 2 through 5 to specify any other search criteria.
7. When finished specifying your search criteria, click **Search**.

   The users who match your search criteria are displayed.

   Alternatively, you can select all users.
8. Click the check box for each user you want to modify.
9. In the Actions area, select the check box for each setting you want to modify for all of the selected users, and then select the appropriate value. See Bulk Provisioning page field descriptions on page 236.
10. Click **Commit**.

### Related links

Adding a user for Avaya Aura Conferencing (AAC) for Turnkey on page 228

Configuring the recording feature for users on page 349

Bulk Provisioning page field descriptions on page 236

## Bulk Provisioning page field descriptions

| Name | Description |
|---|---|
| **Field** | Displays the following fields to search in the user data:<br>• **Login Name**<br>• **Communication Address Handle**<br>• **Communication Address Domain**<br>• **Last Name**<br>• **First Name**<br>• **Profile name**<br>• **Directory Sync Status**: This field has the following options:<br>  - **Pending (sync error or out of filter scope)**<br>  - **Synced from directory**<br>  - **Local user**<br>• **Created (yyyy-mm-dd hh:mm:ss)**<br>• **Video Enabled**<br>• **Recording Enabled**<br>• **Video Class** |
| **Operation** | The particular list of operations depends on the field selected. For example, for text fields, the operations are:<br>• **Starts with**<br>• **Contains**<br>• **Equals**<br>• **After**<br>• **Before**<br>For boolean fields and for the **Directory Sync Status** field, you cannot change the operation. It is always **Equals**. For the **Created (yyyy-mm-dd hh:mm:ss)** field, the options are **After** or **Before**. |
| **Value** | Displays the data to find in the specified user field. |

| Button | Description |
|---|---|
| **Add Criteria** | Adds the information you specified in the **Field**, **Operation**, and **Value** fields into the search criteria list box. |
| **Edit** | Enables you to modify the selected search criteria. |
| **Remove** | Deletes the selected search criteria. |
| **Remove all** | Deletes all the search criteria. |
| **Search** | Searches the user data using the displayed search criteria. |
| **Commit** | Saves the changes. |
| **Export Search Results to CSV** | Exports the search results to a spreadsheet. |

| Name | Description |
|---|---|
| **Directory Distinguished Name column** | Displays an element which operates in conjunction with the search scope.<br>The element is a tree to synchronize users. The domain part of the distinguished name is automatically based on the selected domain and cannot be changed. For example, cn=Users,dc=example,dc=com display. |
| **Login name column** | Displays the login name of each user. |
| **Communication Profile** | Displays the administered communications profile for each user. |
| **Last Name** | Displays the last name of each user. |
| **First Name** | Displays the first name of each user. |

| Name | Description |
|---|---|
| **Conference Profile** | Specifies the conference class of service to assign to the selected users. |
| **Enable Video** | Specifies whether video is enabled or disabled for the selected users. |
| **Enable Recording** | Specifies whether the recording feature is enabled or disabled for the selected users. |
| **Delete User** | Specifies whether to delete all selected users. |

**Related links**

Modifying multiple users at one time on page 235

## Modifying a user's conferencing settings

### Before you begin

You must be logged into Provisioning Client.

### About this task

Use this procedure to modify the conferencing settings for a user.

### Procedure

1. In the Provisioning Client window, select **User Management > Conferencing User**.
2. In the Select login name box, enter the login name for the user. Be sure to include the domain name (for example, yourname@company.com).
3. Click **>>**.
4. Make your changes. See Conferencing User page field descriptions on page 238.
5. Click **Save**.

**Related links**

Adding a user for Avaya Aura Conferencing (AAC) for Turnkey on page 228
Conferencing User page field descriptions on page 238

## Conferencing User page field descriptions

| Name | Description |
|---|---|
| **Select login name** | Enables you to enter the login name of the conferencing user in which you are interested.<br>You must include the domain with the user's login name (for example, jsmith@yourcompany.com). |
| **Select comm profile** | Enables you to select the communications profile for the user. |
| **Class of service** | Displays the conference class of service assigned to this user. |
| **Enable Video** | Specifies whether video is enabled for this user. |
| **Enable Recording** | Specifies whether conference recording is enabled for this user. |
| **Enable operator control** | Specifies whether this user has operator control privileges.<br>**Note:**<br>This setting is not available for an Event conference class of service. |
| **Priority** | Specifies the quality of service this user will receive. The higher the priority setting, the better the service. |

*Table continues…*

| Name | Description |
|---|---|
| | Your choices are:<br>• **Business Critical**: The resolution, frame rate, or quality of sessions will not be reduced during high-usage network conditions. Sessions will proceed with the requested bandwidth at setup.<br>• **High**: The resolution, frame rate, or quality of sessions may be reduced during high-usage network conditions or to accommodate Business Critical users.<br>• **Medium**: The resolution, frame rate, or quality of sessions may be reduced during high-usage network conditions or to accommodate Business Critical and High priority users. Session reduction will occur for Medium priority users before High priority users. Also, session reduction will be greater for Medium priority users than High priority users.<br>• **Low**: Sessions may lose video and fall back to audio-only during high-usage network conditions or to accommodate higher priority users. |
| **Presenter Collaboration code** | Specifies the code that a user must enter to become a presenter during the Event conference.<br>**Note:**<br>This setting is available for an Event conference class of service.<br>This code is set by the Event conference host. |
| **Participant Collaboration Code** | Specifies the participant code that users must enter to log into this user's conference bridge.<br>This value may consist of one to 44 numeric characters |
| **Moderator Collaboration Code** | Specifies the code that this user must enter to log into the conference bridge as a moderator.<br>This value may consist of one to 44 numeric characters |
| **Participant Pass code** | Specifies the code that users must enter if a participant pass code is required for the conference bridge.<br>This value may consist of one to 44 numeric characters |

*Table continues…*

| Name | Description |
|---|---|
| **Moderator Pass code** | Specifies the code that this user must enter if a moderator pass code is required for the conference bridge.<br>This value may consist of one to 44 numeric characters |

**Related links**

Modifying a user's conferencing settings on page 237

# Deleting a user

## Before you begin

- You must be logged into Provisioning Client.
- Your login must have Expert mode privileges to perform this procedure.

⚠ **Warning:**

If you have an Avaya Aura® deployment, any changes you make may cause the Provisioning Client data to become out of sync with the data in Avaya Aura System Manager. You should only modify data to fix sync issues that cannot be resolved from the System Manager interface.

## About this task

Use this procedure to delete a user's Avaya Aura® Conferencing account.

## Procedure

1. In the Provisioning Client window, select **User Management > Search Users**.
2. From the Search by box, select the user criterion you want to search.
3. In the Search for box, enter the appropriate search information for the user.
4. Click **Search**.
5. In the Login name column, click on the Login Name of the user.
6. Click the **Actions** tab.
7. Click **Delete User**.
8. In the Confirmation window, enter your password, and click **Confirm**.

**Related links**

Adding a user for Avaya Aura Conferencing (AAC) for Turnkey on page 228

# Chapter 13: Configuring Avaya Media Servers and clusters

## Software installation procedure for adding additional media servers

The following table provides a high-level view of the tasks involved in configuring and deploying additional media servers.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Download HP documentation | See Downloading HP documentation on page 87 | | |
| 2 | Install hardware | See Installing the server in the rack on page 93 | The hardware requirements for Avaya Aura® Conferencing are the same whether you are installing the product in an Avaya Aura® deployment or a Turnkey deployment. In both cases, it is the HP ProLiant DL360 G9 server. | |
| 3 | Review the prerequisites. | See Prerequisites for software installation on page 119 | | |
| 4 | Configure RAID arrays. | See Managing Hewlett Packard Smart Arrays on page 97 | | |
| 5 | Install the Avaya Aura® Conferencing Platform on the additional server | See Installing the AAC Platform on page 121 | | |
| 6 | Install the Avaya Aura® Media Server platform on the additional server. | See Installing Avaya Media Server  on page 153 | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 7 | Add additional Avaya Aura® Media Server host. | See Adding additional Avaya Media Server hosts on page 242 | | |
| 8 | Add an Avaya Aura® Media Server network element. | See Adding an Avaya Media Server network element on page 243 | | |
| 9 | Deploy an Avaya Aura® Media Server network element. | See Deploying a Network Element instance on page 244 | | |
| 10 | Create a new media server cluster.<br>**Note:**<br>Skip this step if you want to add an additional Avaya Aura® Media Server to an existing media server cluster. | See Creating a new cluster on page 245 | | |
| 11 | Add an additional Avaya Aura® Media Server to media server cluster. | See Adding an additional Avaya Media Server to an existing media server cluster on page 245 | | |

**Related links**

Introduction to software installation on page 110

# Adding additional Avaya Aura® Media Server hosts

## Before you begin

Install the Avaya Aura® Media Server software on a server. For more information, see Installing Avaya Aura Conferencing on page 121.

## About this task

Use this procedure if you want to add expansion Avaya Aura® Media Servers.

## Procedure

1. In the navigation pane of Element Manager Console, click **Addresses**.
2. In the Addresses window, click **Add (+)**.
3. In the Add IPv4 Address dialog box, enter the logical name and IP address for the server on which the Avaya Aura® Media Server software is installed.

4. Click **Apply**.
5. In the navigation pane of Element Manager Console, click **Servers**.
6. In the Servers window, click **Add (+)**.
7. In the Add Server dialog box, complete the following fields:
   - **Short Name**
   - **Long Server Name**
   - **Physical site**
   - **Internal OAM (Default) Address**: Enter the IP address you specified in Step 3.
   - **Operating System**: Select **linux**.
   - **Host Name**: Enter the short name or FQDN of the server.
8. Click **Apply**.

### Next steps

Proceed to Adding an Avaya Aura Media Server network element on page 243.

## Adding an Avaya Aura® Media Server network element

### About this task

Use the following procedure to add an Avaya Aura® Media Server network element.

### Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Media Servers and Clusters > Media Servers**.
2. In the Media Servers window, click **Add (+)**.
3. In the Add Media Server dialog box, complete the following fields:
   - **Short Name**
   - **Long Name**
   - **Base Port**: Type `49000`.
   - **Enable SIP TCP**: Select this check box to enable SIP TCP.

     **OR**

     **Enable SIP TLS**: Select this check box to enable SIP TLS.
   - **SIP Certificate**: If SIP TLS is enabled, select the certificate you want to use for SIP TLS.

     For more information, see Introduction to certificates on page 552.

> **Note:**
>
> Accept the default for all other fields.

4. Click **Apply**.
5. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers** > **<media server you specified in Step 3> Instance**.
6. In the Media Server Instance window, click **Add (+)**.
7. In the Add Media Server Instance dialog box, complete the following fields:
   - **Server**: Select the media server you created in Step 3.
   - **Load or Patch**: Select the software load.
   - **Engineering**: Select the configuration that corresponds to your hardware type and layout.
8. Click **Apply**.

### Next steps

Proceed to Adding an additional Avaya Aura Media Server to an existing media server cluster on page 245.

## Deploying a network element instance

### About this task

Use this procedure to deploy a network element instance.

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements**> ***<Network Element type>*** > ***<Network Element instance you want to deploy*** > **NE Maintenance**.
2. In the Maintenance dialog box, select the row that has a value of the target instance in the ID column.
3. Click **Deploy**.

   The Maint state changes from **None** to **Deploying**, indicating that the deploy operation is in progress. When the deploy operation is complete, the Maint state changes back to **None**, and the Admin state changes from **Configured** to **Offline**.
4. Close the Maintenance window.

### Result

The Network Element instance is deployed.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

## Adding an additional Avaya Aura® Media Server to an existing media server cluster

### About this task

Use the following procedure to add an additional Avaya Aura® Media Server to an existing media server cluster.

### Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Media Servers and Clusters > Media Server Clusters**.
2. In the Media Servers Clusters window, select the media server cluster to which you want to add the Media Server.
3. Click **Edit (-/+)**.
4. In the Edit Media Server Cluster dialog box, specify whether the Media Server you are adding to the cluster is a secondary server (if the cluster has only one Media Server) or a standard media server (if the cluster already has a secondary Media Server).

   **Note:**

   A media server cluster supports a maximum of eight media servers:

   - one primary
   - one secondary
   - six standard servers
5. Click **Apply**.

### Next steps

Proceed to Creating a new Media Server cluster on page 245.

## Creating a new Media Server cluster

### About this task

Use the following procedure to create a new Media Server cluster.

**Note:**

A Media Server cluster supports a maximum of eight Media Servers:

- one primary
- one secondary
- six standard servers

## Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Media Servers and Clusters > Media Server Clusters**.
2. In the Media Server Clusters window, click **Add (+)**.
3. In the Add Media Server Cluster dialog box, complete the following fields:
    - **Short Name**
    - **Long Name**
    - **Primary Server**: Select the Avaya Aura® Media Server network element. This list contains only the media server network elements that do not belong to any cluster. You must specify a primary server.
    - **Secondary Server**: If this cluster has two or more Avaya Aura® Media Servers, you must specify a secondary server. Otherwise, leave this field blank.
    - **Role**:
        - To use this cluster only for the conferencing without recording, choose **CONFERENCING ONLY**.
        - To use this cluster as separated cluster for recording without serving the conferencing choose **RECORDING ONLY**.
        - To use this cluster for recording and conferencing choose **CONFERENCING AND RECORDING**.
    - **Standard Media Servers**: If the cluster has three or more Avaya Aura® Media Servers, add more standard media servers. In the Available box, select the Media Servers you want to add, and then click **>>**.
4. Click **Apply**.

# Chapter 14: Configuring Web Conferencing components

## Configuration procedure for the Web conferencing server components

The following table provides a high-level view of the tasks involved in configuring the Web conferencing components.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Configure the address that appears on the Avaya Aura® Conference Manager Add-in for Microsoft Outlook® notification e-mails. | See Configuring a Web conferencing host on page 226 | | |
| 2 | Deploy the WCMS instances but do not start these instances. | See Deploying and starting the Web conferencing management Network Elements on page 297. | | |
| 3 | Setup Rsync. | See Adding a Web Conferencing Management Server Rsync user account on page 258. | | |
| 4 | Start the Web Conferencing Management Server instances. | See Deploying and starting the Web conferencing management Network Elements on page 297. | | |

**Note:**

Avaya recommends that you implement DNS lookup to synchronize domain names and IP addresses for the Avaya Aura® Conferencing solution. If your deployment does not support DNS lookup, see DNS and Avaya Aura Conferencing on page 671.

# Configuring a Web conferencing host

This task is particularly significant if you plan to deploy the Avaya Aura® Conference Manager Add-in for Microsoft Outlook®. You will require the Web conferencing host name during the configuration of the Avaya Aura® Conference Manager Add-in for Microsoft Outlook®.

### About this task

Use the following procedure to configure a Web conferencing host name.

### Procedure

1. In the Provisioning Client window, select **System Management** > **Routing** > **Collaboration Agent Service FQDN**.
2. In the FQDN field, enter an FQDN name.

   Depending on the deployment type, you should enter either:

   - The fully qualified domain name (FQDN) of the Provisioning Manager network element/ Collaboration Agent network element.
   - The FQDN of the load balancer.
3. Click **Save**.

**Related links**

Deploying the Avaya Aura Conference Manager Add-in for Microsoft Outlook on page 622
Implementing a ClickOnce deployment on page 623
Implementing a centralized software deployment on page 625

# Configuring the meeting event processor for the Web conferencing management server

### About this task

Use the following procedure to configure the meeting event processor.

### Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Web Conferencing > Web Conferencing Management > Web Conferencing Management Servers ><*Web conferencing management server name*> > Meeting Event Processing**.
2. From the Meeting Event Processor box, select the Provisioning Manager or Collaboration Agent for managing meeting events.
3. Click **Apply**.

# Web Conferencing Server (WCS) clusters

Within the Avaya Aura® Conferencing environment, the concept of a 'cluster' provides a mechanism for Avaya Aura® Conferencing administrators to provision a collection of servers as one single server. This mechanism reduces the number of configuration tasks but also maximizes load balancing between the servers. In this release, Avaya Aura® Conferencing supports the concept of a media server (MS) cluster and a Web Conferencing Server (WCS) cluster. In this Avaya Aura® Conferencing release, WCS clusters replace WCS groups from previous releases.

When Avaya Aura® Conferencing chooses which WCS cluster to use for a particular conference, it uses the following process:

- Avaya Aura® Conferencing checks if there is a WCS cluster provisioned to serve the user (conference owner) in their location.
- If there are no WCS clusters available in the same location as the user, Avaya Aura® Conferencing searches for WCS clusters serving the user's location, and selects the least loaded WCS from amongst those clusters.
- If there are still no WCS available, Avaya Aura® Conferencing uses the default WCS cluster.

There are additional options available if you wish to ensure that users from a particular location use the system resources in another location.

Avaya Aura® Conferencing follows this process:

- When it chooses which WCS to use for hosting a conference.
- When it chooses which WCS to use for recording a conference.
- When it chooses which WCS to use for playing back a conference.
- When it chooses which WCS to use for encoding a conference that does not include web collaboration.

Encoding, within this context, refers to the process of processing a conference recording to convert it to a playable format. If the conference contains web collaboration, Avaya Aura® Conferencing uses the hosting server for the encoding process.

You must also provision dedicated WCS clusters if you wish to support event conferences. For more information about event conferences, see Event conferencing and media cascading on page 45.

**Related links**

WCS clusters and the upgrade process on page 250
WCS clusters and Application Delivery Controller (ADC) functionality on page 250
Creating a new WCS cluster on page 250
Configuring the default cluster on page 251
Assigning WCS clusters to serving locations on page 252
Assigning WCS clusters to physical locations on page 253
Assigning WCS clusters to hosting locations on page 255
Configuring WCS clusters for event conferences on page 256
Both deployments on page 347

## WCS clusters and the upgrade process

During the upgrade process from previous Avaya Aura® Conferencing releases to this Avaya Aura® Conferencing release, Avaya Aura® Conferencing creates a WCS cluster for each WCS in your deployment. After the upgrade is complete, you must combine the WCS clusters into an appropriate configuration for your deployment. Additionally, if your deployment supports event conferencing, in most cases, you must manually re-configure and re-assign the appropriate WCS clusters for event conferences. The only exception to this rule is if your deployment consists of a single WCS cluster for event conferencing and this WCS cluster is only assigned to a single location.

**Related links**

Web Conferencing Server (WCS) clusters on page 249

## WCS clusters and Application Delivery Controller (ADC) functionality

Avaya Aura® Conferencing supports the A10 Network AX Series Application Delivery Controller and the Barracuda Load Balancer Application Delivery Controller, which provide advanced load balancing as well as reverse proxies for Web Collaboration as well as for the Audio/Video in Collaboration Agent clients.

If your deployment supports a reverse proxy controller that uses web sockets[8], you must enter a WCS service address in the **Cluster FQDN** field on the **Add Web Conferencing Server Cluster** dialog when you are creating a new WCS cluster. The WCS Cluster Service address/Cluster FQDN is the fully qualified domain name of the WCS cluster.

For more information about the **Add Web Conferencing Server Cluster** dialog, see Creating a new WCS cluster on page 250.

For more information about the configuration of WCS clusters for the reverse proxy, see Configuring the WCS virtual service for WCS clusters on page 414.

**Related links**

Web Conferencing Server (WCS) clusters on page 249

## Creating a new WCS cluster

### About this task

Use the following procedure to create a new Web Conferencing Server (WCS) cluster.

[8] WebSocket is a protocol providing full-duplex communications channels over a single TCP connection.

**Note:**

A WCS can only be a member of a single WCS cluster.

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Servers and Clusters** > **Web Conferencing Server Clusters**.
2. In the Web Conferencing Server Clusters window, click **Add (+)**.
3. In the Add Web Conferencing Server Cluster dialog box, complete the following fields:
   - **Short Name**
   - **Long Name**
   - **Cluster FQDN**: If your deployment includes a reverse proxy server, you must enter a value in this field. If your deployment does not include a reverse proxy server, you must leave this field blank. Avaya supports the A10 Application Delivery Controller for reverse proxy functionality in Avaya Aura® Conferencing.
4. From the **Available** panel, select a WCS.
5. Click the arrow **>>** button.

   The WCS is displayed in the **Used** panel and becomes a member of the WCS cluster.
6. Repeat these steps to add additional WCSs to the cluster.
7. Click **Apply**.

#### Related links

Web Conferencing Server (WCS) clusters on page 249

## Configuring the default cluster

Avaya Aura® Conferencing uses a default WCS cluster if there is no cluster assigned to a location or if there are no system resources available on the assigned WCS clusters.

### Before you begin

Create at least one WCS cluster. See Creating a new cluster on page 250.

### About this task

Use this task to configure a default WCS cluster.

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Servers and Clusters** > **Default Web Conferencing Server Cluster**.
2. In the Default Web Conferencing Server Cluster window, select a value from the Default Web Conferencing Server Cluster drop-down list.

3. Click **Ok**.

### Related links

Web Conferencing Server (WCS) clusters on page 249

## Assigning WCS clusters to serving locations

### Before you begin

- You must be logged into Provisioning Client.
- Create at least one WCS cluster. See Creating a new cluster on page 250.
- Configure at least one location. See Adding a location on page 223.

### About this task

If your deployment contains only one WCS cluster, you simply need to configure a default WCS cluster. However, if your deployment contains multiple WCS clusters, you must assign the WCS clusters to a serving location for communication with other network elements. Use the following procedure to assign a particular WCS server cluster to a location.

### Procedure

1. In the Provisioning Client window, select **System Management** > **Routing** > **Web Conferencing Server Resources**.
2. Click the **WCS cluster/DCS serving locations** tab.
3. Select a location from the **Location** drop-down list.
4. From the **Available WCS Clusters** box, select the appropriate WCS server cluster, and then click **Copy**. If you want to assign all available WCS server clusters, click **Copy all**.
5. Click **Save**.
6. Repeat Steps 3 through 6 for each location.

### Related links

Web Conferencing Server (WCS) clusters on page 249
WCS cluster/DCS serving locations tab field descriptions on page 252

## WCS cluster/DCS serving locations tab field descriptions

| Name | Description |
|---|---|
| **Location** | For any Location you have configured on System Manager, you must add it manually to Provisioning Client. A location can be a physical site office location or a virtual collective of users. |
| **Available WCS Clusters** | Displays a list of provisioned WCS clusters. |

*Table continues…*

| Name | Description |
|---|---|
| **Selected WCS Clusters** | Displays the WCS servers assigned to the selected WCS cluster. |
| **Document Conversion Server** | If there is a Document Conversion Server (DCS) assigned to this location, it is displayed here. |

| Button | Description |
|---|---|
| **Copy all** | Moves all of the WCS servers displayed in the **Available WCS Clusters** box to the **Selected WCS Clusters** box. |
| **Copy** | Moves the selected WCS server displayed in the **Available WCS Clusters** box to the **Selected WCS Clusters** box. |
| **Remove** | Moves the selected WCS server in the **Selected WCS Clusters** box to the **Available WCS Clusters** box. |
| **Remove all** | Moves all of the WCS servers displayed in the **Selected WCS Clusters** box to the **Available WCS Clusters** box. |
| **Save** | Click **Save** to apply your changes. |

### Related links

Assigning WCS clusters to serving locations on page 252

## Assigning WCS clusters to physical locations

When Avaya Aura® Conferencing chooses a WCS cluster, it checks the WCS clusters configured for the serving location of the conference. If there are several suitable WCS clusters available in the serving location, Avaya Aura® Conferencing checks the WCS clusters configured for the physical location of the conference.

### Before you begin

- You must be logged into Provisioning Client.
- Create at least one WCS cluster. See Creating a new cluster on page 250.
- Configure at least one location. See Adding a location on page 223.

### About this task

Use the following procedure to assign a particular WCS server cluster to a physical location.

### Procedure

1. In the Provisioning Client window, select **System Management** > **Routing** > **Web Conferencing Server Resources**.
2. Click the **WCS Cluster Physical Location** tab.

You can select WCS servers associated with a particular location or you can select WCS servers associated with a particular WCS cluster.

3. Choose a selection criteria.
    - If you choose to select from the WCS servers associated with a particular location, select **Location** from the **Select By** list. Provisioning Client displays a list of the WCS servers associated with that location in the **Select Physical Location** list.
    - If you choose to select from the WCS servers associated with a particular WCS cluster, select **WCS Cluster** from the **Select By** list. Provisioning Client displays a list of the WCS servers associated with that WCS cluster in the **Select Web Conferencing Cluster** list.
4. From the **Available WCS Clusters** box, select the appropriate WCS server cluster, and then click **Copy**. If you want to assign all available WCS server clusters, click **Copy all**.
5. Click **Save**.
6. Repeat Steps 3 through 6 for each location.

**Related links**

Web Conferencing Server (WCS) clusters on page 249

WCS Cluster Physical Location tab field descriptions on page 254

## WCS Cluster Physical Location tab field descriptions

| Name | Description |
|---|---|
| **Select by** | Displays the two selection criteria for choosing a WCS. You can choose from a list of WCSs assigned to a location or a list of WCSs assigned to a WCS cluster. |
| **Select Physical Location** | Displays a list of the locations of WCSs. |
| **Select Web Conferencing Cluster** | Displays a list of the provisioned WCS clusters. |
| **Available WCS Clusters** | Displays a list of provisioned WCS clusters. |
| **Selected WCS Clusters** | Displays the WCS servers assigned to the selected WCS cluster. |

| Button | Description |
|---|---|
| **Copy all** | Moves all of the WCS servers displayed in the **Available WCS Clusters** box to the **Selected WCS Clusters** box. |
| **Copy** | Moves the selected WCS server displayed in the **Available WCS Clusters** box to the **Selected WCS Clusters** box. |
| **Remove** | Moves the selected WCS server in the **Selected WCS Clusters** box to the **Available WCS Clusters** box. |

*Table continues…*

| Button | Description |
|---|---|
| **Remove all** | Moves all of the WCS servers displayed in the **Selected WCS Clusters** box to the **Available WCS Clusters** box. |
| **Save** | Click **Save** to apply your changes. |

**Related links**

Assigning WCS clusters to physical locations on page 253

## Assigning WCS clusters to hosting locations

You may wish to assign an alternative location to a particular group of users residing in a particular location. For example, your deployment may consist of a primary office site and a secondary office site. You may want the users in the secondary office site to use the Avaya Aura® Conferencing system resources from the primary office site. In other words, you may want the WCS cluster in the primary site to host a conference initiated by a user from the secondary site. You can use the concept of a hosting location to implement this functionality.

### Before you begin

- You must be logged into Provisioning Client.
- Create at least one WCS cluster. See Creating a new cluster on page 250.
- Configure at least one location. See Adding a location on page 223.

### About this task

Use this task to configure an alternative location for conferences.

### Procedure

1. In the Provisioning Client window, select **System Management** > **Routing** > **Web Conferencing Server Resources**.
2. Click the **Hosting Locations** tab.
3. Select a hosting location from the **Select Hosting Location** list.

   For example, select a primary office site.
4. From the **Hostable Locations** box, select the appropriate location, and then click **Copy**. If you want to assign all available locations, click **Copy all**.

   For example, select a secondary office site.
5. Click **Save**.
6. Repeat Steps 3 through 6 for each location.

**Related links**

Web Conferencing Server (WCS) clusters on page 249

## Hosting Locations tab field descriptions

| Name | Description |
|---|---|
| **Select Hosting Location** | Displays the hosting location. This location will host the conferences for the locations listed in the **Hosted Locations** box. |
| **Hostable Locations** | Displays a list of provisioned locations. |
| **Hosted Locations** | Displays the locations assigned to the selected hosting location. |

| Button | Description |
|---|---|
| **Copy all** | Moves all of the locations displayed in the **Hostable Locations** box to the **Hosted Locations** box. |
| **Copy** | Moves the selected location displayed in the **Hostable Locations** box to the **Hosted Locations** box. |
| **Remove** | Moves the selected location in the **Hosted Locations** box to the **Hostable Locations** box. |
| **Remove all** | Moves all of the locations displayed in the **Hosted Locations** box to the **Hostable Locations** box. |
| **Save** | Click **Save** to apply your changes. |

# Configuring WCS clusters for event conferences

Event conferences are very large conferences that are used for gathering 100s or possibly 1000s of participants, often from multiple global locations. Event conferences are used for company announcements, town hall meetings, and so on. For more information about event conferences, see Event conferencing and media cascading on page 45 and Event conferencing considerations on page 54.

To configure event conferencing correctly, you must:

- Create and configure a WCS cluster that is dedicated to event conferencing, as described here.
- Assign a physical location to the WCS cluster, using the procedure in Assigning clusters to physical locations on page 253.
- Assign a user to the event location, using the procedure in Adding a user from Provisioning Client on page 229.
- Configure a media server cluster, as described in Configuring Event conferencing on page 332.

### Before you begin

- You must be logged into Provisioning Client.

- Create at least one WCS cluster. See Creating a new cluster on page 250.
- Configure at least one location. See Adding a location on page 223.

### About this task

Use this task to configure a dedicated WCS cluster for event conferencing.

### Procedure

1. In the Provisioning Client window, select **System Management** > **Routing** > **Web Conferencing Server Resources**.
2. Click the **WCS Clusters for Event Conference** tab.
3. From the **Available WCS Clusters** box, select a WCS cluster, and then click **Copy**. If you want to assign all available WCS clusters, click **Copy all**.
4. Click **Save**.

#### Related links

Web Conferencing Server (WCS) clusters on page 249
WCS Clusters for Event Conference tab field descriptions on page 257
Configuring media server clusters for event conferences on page 332
WCS Clusters for Event Conference tab field descriptions on page 257
Event conferencing and media cascading on page 45

## WCS Clusters for Event Conference tab field descriptions

| Name | Description |
|---|---|
| **Available WCS Clusters** | Displays a list of clusters that are not assigned as serving a location for non-event conferences. |
| **Selected WCS Clusters** | Displays the WCS servers assigned to the selected WCS cluster. |

| Button | Description |
|---|---|
| **Copy all** | Moves all of the locations displayed in the **Available WCS Clusters** box to the **Selected WCS Clusters** box. |
| **Copy** | Moves the selected location displayed in the **Available WCS Clusters** box to the **Selected WCS Clusters** box. |
| **Remove** | Moves the selected location in the **Selected WCS Clusters** box to the **Available WCS Clusters** box. |
| **Remove all** | Moves all of the locations displayed in the **Selected WCS Clusters** box to the **Available WCS Clusters** box. |
| **Save** | Click **Save** to apply your changes. |

# Configuring Web Conferencing Management Server Rsync

This section provides information about creating a new rsyncappsw user, a Secure Shell (SSH) key, and transferring a copy of the SSH key to the server when multiple Web Collaboration Management Server (WCMS) instances are running.

### Before you begin

- A Web Conferencing Management Server instance on each server must be deployed but not started. The following procedures refer to the servers as ServerA and ServerB.

  **Note:**

  ServerA is the server where the WCMS1 instance is configured and ServerB is the server where the WCMS2 instance is configured.

- You are able to log on using the ntsysadm account or an account with the SA role assigned.

**Related links**

Adding a Web Conferencing Management Server Rsync user account on page 258

Generating an SSH user key on page 259

Copying the SSH key on page 259

## Adding a Web Conferencing Management Server Rsync user account

### Procedure

1. Log on to the server through ssh as ntsysadm or an account with the SA role assigned.
2. Type **`userMgt`**, and press **Enter**.
3. Type `1`, and press **Enter** to add new user.
4. At the prompt to enter a username, type `rsyncappsw`, and press **Enter**.
5. At the prompt to enter a user ID (between 1000 and 10000), type a number or press **Enter** to have the system select an ID for you.
6. Type `5` to select the AA role, and press **Enter**.
7. Type `y`, and press **Enter** to continue.
8. At the prompt to Enter a new password, type a password, for example, `ZAQ12wsx`, and press **Enter**.
9. At the prompt to add another user, press **Enter** to skip adding another user.
10. Press **Enter** to exit the userMgt tool.
11. Type `sudo chage --maxdays -1 rsyncappsw`, and press **Enter**.

### Next steps

Proceed to generating a user key or return to the Checklist for configuring the Web conferencing server components on page 247 to determine where you are in the process..

#### Related links

Configuring Web Conferencing Management Server Rsync on page 258

## Generating an SSH user key

### Procedure

1. Type `cd /var/mcp/run/MCP_18.X/<WCMS1_0>/bin`, and press **Enter** to go to the WCMS instance runtime bin directory.

   Where: WCMS1_0 is Server A and WCMS2_0 is Server B.
2. Type **`sudo -u rsyncappsw ./genSSHUserKeys.sh`**, and press **Enter**.

   A new key is generated.
3. Type **`sudo su - rsyncappsw`**, and press **Enter**.
4. Type **`passwd`**, and press **Enter**.
5. Type the old password, as entered in the preceding procedure, for example `ZAQ12wsx`, and press **Enter**.
6. Type a new password at the prompt, and press **Enter**.
7. Retype the new password at the prompt, and press **Enter**.
8. Log on to ServerB through ssh as `ntsysadm` or an account with the SA role assigned
9. Repeat the steps in Adding a Web Conferencing Management Server Rsync user account on page 258 and Generating an SSH user key on page 259 for ServerB.

### Result

A new key is generated for ServerA and ServerB.

### Next steps

Proceed to transferring a copy of the SSH key or return to the Checklist for configuring the Web conferencing server components on page 247 to determine where you are in the process.

#### Related links

Configuring Web Conferencing Management Server Rsync on page 258

## Copying the SSH key

### About this task

Transfer a copy of the SSH key to the servers where the WCMS instances are running.

### Procedure

1. Log on to ServerA through ssh as `ntsysadm` or an account with the SA role assigned.
2. Type **`sudo -u rsyncappsw ssh-copy-id -i /home/rsyncappsw/.ssh/id_rsa.pub <ServerB_IP>`**, and press **Enter**.

   The following prompt appears:

   ```
   Are you sure you want to continue connecting (yes/no)?
   ```
3. Type `y` and press **Enter**.
4. At the prompt to enter a password, type the password that you specified when you generated the SSH user key, and press **Enter**.

   The command succeeded if you see `Now try logging into the machine, with "ssh '<IP address>'", and check in:`

   ```
   .ssh/authorized_keys
   ```

   ```
   to make sure we haven't added extra keys that you weren't
   expecting.
   ```
5. Log off ServerA.
6. Log on to ServerB through ssh as `ntsysadm` or an account with the SA role assigned.
7. Repeat Step 2 on page 260 and replace <ServerB_IP> with <ServerA_IP> and continue through to Step 5 on page 260.
8. Log off ServerB.

### Next steps

Return to step 9 in the Checklist for configuring the Web conferencing server components on page 247.

#### Related links

Configuring Web Conferencing Management Server Rsync on page 258

## Migrating to and from a DMZ

In an SMB or medium deployment, the Avaya Aura® Conferencing components are deployed on the Element Manager servers. If you want to offer Web collaboration features to participants outside of the enterprise, you must configure an Application Delivery Controller (ADC) using any of the supported Delivery Controllers. For more information, see chapter “Configuring an Application Delivery Controller (ADC)”.

You can also use the legacy option and move the Web Conferencing components to a separate server in the Demilitarized Zone (DMZ). The following migration options are available:

| From | To |
|---|---|
| SMB or medium simplex layout | SMB or medium simplex with DMZ layout |
| SMB or medium with redundancy layout | SMB or medium with redundancy with DMZ layout |

Using the following sections, you can also migrate back from a DMZ deployment to a deployment without a DMZ. If you have a medium simplex layout, use the large OVA for a dedicated Avaya Aura® Conferencing Web server in the DMZ.

**Related links**

Checklist for migrating to a DMZ on page 261
Migrating the Web Conference Server to the DMZ on page 262
Migrating the Web Conference Server from the DMZ on page 264
Enterprise DMZ deployment on page 45

## Checklist for migrating to a DMZ

The following table provides a high-level view of the tasks involved in migrating to a DMZ.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Ensure that you have the appropriate hardware configuration required for this deployment. | See Deployment layouts on page 34. | | |
| 2 | Install the appropriate software on the DMZ server. Ensure that you apply the appropriate patches. | See Installing the AAC Platform on page 121.<br>**Important:**<br>The procedure guides you through the installation process with links to individual procedures. Upon completion of each step, return to the next step in the Installing Linux procedure by clicking the link at the end of each individual procedure. | | |
| 3 | Configure the firewall rules on the DMZ server. | For information about the port matrix, go to http://support.avaya.com and | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| | | download the latest version of the Avaya Aura® Conferencing Port Matrix. | | |
| 4 | Configure the access control list on the DMZ server. | See Configuring the access control list on page 601. | | |
| 5 | Migrate the Web conferencing components from the Element Manager servers in the enterprise to the separate servers, located in the DMZ. | See Migrating the web conference server to the DMZ on page 262. | | |

**Related links**

Migrating to and from a DMZ on page 260

# Migrating the Web Conference Server to the DMZ

## About this task

If you have an SMB or medium deployment, use this task to move the Web Conferencing components from the Element Manager server to a separate server located in the DMZ. If your SMB or medium deployment has redundancy, perform all of the steps for one Element Manager server and Web Conferencing server and then perform the steps for the second Element Manager server and Web Conferencing server.

## Procedure

1. Stop all instances of the Web Conferencing Management Server (WCMS), Web Conferencing Server (WCS), and Provisioning Management (PROV) network elements (NE).
2. Undeploy the WCS NE instances.

   See Stopping and undeploying a network element instance on page 628.
3. Add the WCS OAM addresses:
   a. In the navigation pane of Element Manager Console, select **Addresses**.
   b. In the Addresses window, click **Add (+)**.
   c. In the Add IPv4 Address dialog box, complete the following fields:
      - **Logical Name**
      - **IPv4 Address**

   d. Click **Apply**.

   e. Click **Yes** to confirm.
   f. Repeat this procedure for any additional WCS.

4. Change the WCS service addresses to the free IP addresses that belong to the WCS located in the DMZ.
   a. In the navigation pane of Element Manager Console, select **Addresses**.
   b. In the Addresses window, select the WCS service address and click **Edit (-/+)**.
   c. In the Edit IPv4 Address dialog box, change the IP address in the **IPv4 Address** field.
   d. Click **Apply**.
   e. Repeat this procedure for any additional WCS.
5. Add the WCS:
   a. In the navigation pane of Element Manager Console, select **Servers**.
   b. In the Servers window, click **Add (+)**.
   c. In the Add Server dialog box, complete the following fields:
      - **Short Name**
      - **Long Server Name**
      - **IPv4 Internal OAM (Default) Address**: Enter the IP address you specified in Step 3.
      - **Operating System**: Select **linux**.
   d. Click **Apply**.
   e. Repeat this procedure for any additional WCS.
6. Change the servers for the WCS NE instances to Web Conferencing servers.

   For example, in an SMB or medium simplex (without redundancy) deployment, change the WCS NE instance to WCServer1.

   a. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Servers and Clusters** > **Web Conferencing Servers** > **<WCS NE>** > **Instance**.
   b. In the <WCS> Instance dialog box, select the WCS NE instance.
   c. Click **Edit (-/+)**.
   d. In the Edit <WCS> Instance dialog box, select the WCS from the **Server** list.
   e. Click **Apply**.
   f. Repeat this procedure for any additional WCS.
7. Add Collaboration Agent Network Element (CA NE) instances.
   a. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Collaboration Agent Managers** > **<CA NE>** > **Instance**.

   b. In the <CA NE> Instance dialog box, click **Add (+)**.
   c. Select the Web Conferencing server and click **Apply**.
   d. Select the appropriate engineering profile from the **Engineering** drop-down list.
   e. Repeat this procedure for any additional WCS.

8. Deploy the WCS and CA NE instances.

   See Deploying a Network Element instance on page 244.

9. Ensure that the WCS Service address is in the same subnet as the WC servers.

10. Change the certificates configured for WCS and CA NEs in accordance with Guidelines for certificate configuration on page 566.

    See Automated security on page 555.

11. Start all stopped Web Conferencing Management Server (WCMS), Web Conferencing Server (WCS), Collaboration Agent (CA) and Provisioning Management (PROV) Network Element instances.

    See *Deploying and starting the remaining Network Elements*.

**Related links**

Migrating to and from a DMZ on page 260

## Migrating the Web Conference Server from the DMZ

### About this task

If you have an SMB or medium deployment, use this task to move the Web Conferencing components from a separate server located in the DMZ to the Element Manager server. If your an SMB or medium deployment has redundancy, perform all of the steps for one Element Manager server and Web Conferencing server and then perform the steps for the second Element Manager server and Web Conferencing server.

### Procedure

1. Stop all instances of the Web Conferencing Management Server (WCMS), Web Conferencing Server (WCS), Collaboration Agent (CA) and Provisioning Management (PROV) network elements (NE).

2. Undeploy the WCS NE instances.

   See Stopping and undeploying a network element instance on page 628.

3. Change the servers for the WCS NE instances to Element Manager servers.

   For example, in an SMB or medium simplex (without redundancy) deployment, change the WCS NE instance to EMServer1.

   a. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Servers and Clusters** > **Web Conferencing Servers** > **<WCS NE>** > **Instance**.

   b. In the <WCS> Instance dialog box, select the WCS NE instance.
   c. Click **Edit (-/+)**.
   d. In the Edit <WCS> Instance dialog box, select the Element Manager server from the **Server** list.
   e. Click **Apply**.
   f. Repeat this procedure for any additional WCS.
4. Delete the Collaboration Agent Network Element (CA NE) instances.
   a. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Collaboration Agent Managers (Collaboration Agent Managers)** > **<CA NE>** > **Instance**.
   b. In the <CA NE> Instance dialog box, click **Delete (-)**.
   c. Click **Yes** to confirm.
   d. Repeat this procedure for any additional WCS.
5. Ensure that the WCS Service address is in the same subnet as the EM servers.
6. Change the certificates configured for WCS in accordance with Guidelines for certificate configuration on page 566.

   See Automated security on page 555.
7. Start all stopped Web Conferencing Management Server (WCMS), Web Conferencing Server (WCS), Collaboration Agent (CA) and Provisioning Management (PROV) Network Element instances.

   See Deploying and starting the remaining network elements on page 288.

**Related links**

Migrating to and from a DMZ on page 260

# Chapter 15: Installing or upgrading a Document Conversion Server

## The Document Conversion Server (DCS) in Avaya Aura® Conferencing

> **Note:**
>
> If you have a large Avaya Aura® Conferencing deployment, you must host the Document Conversion Server (DCS) on a separate server. If you have an SMB or medium Avaya Aura® Conferencing deployment, the DCS can reside on the same server as other network elements in the Avaya Aura® Conferencing solution.

For this release, Avaya is deploying the Document Conversion Server (DCS) as a Network Element on the Linux platform.

The DCS is required for sharing documents during Avaya Aura® Conferencing conferences. Linux is a UNIX-like, open-source, operating system. Linux is the leading operating system on most servers.

For this release, Avaya will no longer support the DCS on a Windows operating system. As a result, if you have an existing older Avaya Aura® Conferencing system, you must migrate the DCS from the Windows operating system to the Linux operating system.

You can repurpose/reuse the existing Windows server by installing the Linux operating system and Avaya Aura® Conferencing on it. You can now use this server as a DCS. For SMB and medium deployments, you have the choice of placing the DCS on the same server hosting the other network elements, or having it on its own server. For large deployments, the DCS must always be on its own server.

### HTTPS

Currently, Avaya only supports HTTPS connections to the DCS. As a result, you must generate and assign a certificate for each DCS Network Element.

### Automatic migration

Avaya has automated most of the DCS migration tasks. All existing DCS data elements automatically convert to new DCS Network Elements data objects. Similarly, all current configuration settings, such as location mapping, automatically convert to the new platform.

### Manual tasks

There are still a limited number of tasks that you must manually perform. This is particularly the case if you have a deployment that includes redundancy. Redundancy operates by replicating the database on a standby server. If you have a redundant deployment, for the purposes of the DCS migration, you must stop the replication process for the duration of the migration. You must restart the replication process when the migration has completed. The number and order of the manual tasks varies depending on whether you want to reuse the old/existing DCS Windows server. Choose one of the following tables in accordance with your plans and complete each of the tasks in order.

**Table 20: If you intend to repurpose the existing DCS Windows server as the new DCS Linux server**

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | If your deployment includes redundancy, stop the replication process. | See Dropping the database replication on page 268 and Setting the database type to single on page 269 | | |
| 2 | Stop the existing DCS. | See Stopping the existing DCS on page 268 | | |
| 3 | On the old/existing server, install Linux and Avaya Aura® Conferencing. | See Installing Linux and Avaya Aura Conferencing on page 270 | | |
| 4 | Deploy and start the new DCS. | See Deploying and starting the new DCS on page 270 | | |
| 5 | If your deployment includes redundancy, restart replication. | See Setting up the database replication on page 274 | | |

**Table 21: If you intend to place the new DCS alongside an existing Network Element**

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | If your deployment includes redundancy, stop the replication process. | See Dropping the database replication on page 268 and Setting the database type to single on page 269 | | |
| 2 | Deploy and start the new DCS. | See Deploying and starting the new DCS on page 270 | | |
| 3 | If your deployment includes redundancy, restart replication. | See Setting up the database replication on page 274 | | |

# Stopping an existing DCS

### About this task

Use this task to stop the existing DCS.

### Procedure

1. Login to the DCS Windows server.
2. Stop the DCS by closing the command window that is opened when the DCS is started.

   Alternatively, you can:

   - Press `Ctrl+C`.
   - Type `y`.
   - Press **Enter**.

   The DCS is stopped.
3. Shutdown the Windows server.

**Related links**

Dropping the database replication on page 268
Setting the database type to single on page 269

# Dropping the database replication

### Before you begin

If the **Replication** tab is not immediately displayed, you can press the **Start Monitor** button to display it.

### About this task

Use the following procedure to drop database replication

### Procedure

1. Log in to Element manager Console.
2. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Database** > **<Database name>** > **Monitor**.
3. In the Database Instance Monitor window, go to the **Replication** tab.
4. Ensure that **Incoming Batches** and **Outgoing Batches** have 0 values for **Processing** and **Errors**.
5. Close the Database Instance Monitor window.
6. Log on to the primary Element Manager server as `ntdbadm` or an account with the DBA role.

7. Type `cd /var/mcp/run/MCP_18.X/mcpdb_0/bin/util` and press **Enter**.
8. Type `./cleanupReplication.pl` and press **Enter**.

   The system displays the following information:

   ```
   You are about to drop replication between the 2 Databases.
   This will put both  Databases into a "single mode", and changes will not be
   replicated between them.
   Please Confirm (Y/N): [N]
   ```

9. Type `y`, and press **Enter**.

   The system displays the following information:

   ```
   Cleaning up PRIMARY DB replication
   Cleaning up replication on PRIMARY completed successfully.
   Cleaning up SECONDARY DB replication
   Cleaning up replication on SECONDARDY database completed successfully..
   cleanupReplication.pl Completed at
   ```

### Result

Database replication is dropped.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

**Related links**

Stopping an existing DCS on page 268

## Setting the database type to single

In a redundant deployment, a database on the primary side is replicated to the secondary side. This replication process means that the database is copied so that, in the unlikely event of the primary server going offline, Avaya Aura® Conferencing maintains a copy of all conferencing account information.

This task temporarily disables the replication process during the upgrade. At the end of the upgrade, you must restart the process by setting the database type to REPLICATED.

### About this task

Use this procedure to set the database type to single.

### Procedure

1. Log into the primary Element Manager server as `ntappadm` user.
2. At the prompt, type `populateInstallpropsFile.pl` and press **Enter**.
3. At all the prompts with the exception of **Database Type (SINGLE/REPLICATED)?**, retain the existing values.
4. At the **Database Type (SINGLE/REPLICATED)?** prompt, type `SINGLE` and press **Enter**.

### Result

The database type is set to single.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

**Related links**

Stopping an existing DCS on page 268

## Installing Linux and Avaya Aura® Conferencing

You must install the Avaya Aura® Conferencing platform on the DCS server. For more information, see Installing the AAC platform on page 121.

## Deploying and starting the new DCS

### Before you begin

You must have access to a server on which Linux and Avaya Aura® Conferencing are installed.

You must know which deployment type applies to your situation. There are three types of deployment. These deployment types depend on the size of your enterprise and the extent of your conferencing needs. For more information, see Deployment layouts on page 34.

### About this task

Use this task to deploy and start the new DCS

### Procedure

1. Configure the DCS IP address.

   If you are placing the new DCS alongside an existing Network Element, see Using an existing IP address for the DCS on page 271.

   If you are repurposing/reusing the existing DCS Windows server as the new DCS Linux server, see Assigning a new IP address to the DCS on page 272

2. Configure a security certificate for the DCS.

   Currently, the DCS only supports HTTPS connections. As a result, a security certificate is required. For more information, see Assigning a new certificate to the DCS on page 272.

3. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Document Conversion Servers** > **Document Conversion Servers**.

4. Select the DCS, for example, **DCS1**.
5. Select **Instance**.
6. On the **DCS Instance** dialog, select the DCS instance and click **Edit (-/+)**.
7. On the **Edit DCS Instance** dialog, from the **Server** drop-down menu, select a server.

   This server must have Linux and Avaya Aura® Conferencing installed.
8. From the **Engineering** drop-down menu, select a deployment type.

   There are three types of deployment: SMB, Medium, or Large.
9. Click **Apply**.
10. Start the DCS.

    For more information, see Starting the new DCS on page 273.

### Result

The DCS is now configured.

**Related links**

Using an existing IP address for the DCS on page 271
Assigning a new IP address to the DCS on page 272
Importing a new certificate for the DCS on page 272
Starting the new DCS on page 273
Setting up the database replication on page 274

## Using an existing IP address for the DCS

### About this task

Use this task to assign an existing IP address to the DCS. For example, if you want to place the DCS in an SMB or medium deployment on the same server as another Network Element.

### Procedure

1. In the navigation pane of Element Manager Console, select **Addresses**.
2. Select the DCS and click **Edit (-/+)**.
3. Enter the IP address that you want to assign to the DCS and click **Apply**.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

**Related links**

Deploying and starting the new DCS on page 270

## Assigning a new IP address to the DCS

### About this task

Use this task to assign a new IP address to the DCS. For example, if you have converted the old DCS Windows server to Linux and intend to use it as the new DCS.

### Procedure

1. In the navigation pane of Element Manager Console, select **Addresses**.
2. On the **Addresses** dialog, select the DCS and click **Add (+)**.
3. Enter the IP address that you want to assign to the DCS and click **Apply**.
4. In the **Logical Name** field, enter a name for the DCS.
5. In the **IPv4 Address** field, enter the new IP address.
6. In the navigation pane of Element Manager Console, select **Servers**.
7. On the **Servers** dialog, click **Add (+)**.
8. Complete the fields on the **Add Server** dialog and click **Apply**.

   Ensure that you enter the new IP address in the **IPv4 Internal OAM (Default) Address** field.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

#### Related links

Deploying and starting the new DCS on page 270

## Importing a new certificate for the DCS

### Before you begin

- A new certificate for the Document Conversion Server (DCS) must exist in the Element Manager Keystore.
- The certificate has been signed by a Certificate Authority that is in the Element Manager Truststore. This is typically the System Manager Certificate Authority.

### About this task

Use the following procedure to assign a new certificate to the DCS.

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Document Conversion Servers** > **Document Conversion Servers**.

2. In the Document Conversion Servers window, select the DCS, for example, **DCS1**.
3. Click **Edit (-/+)**.
4. In the Edit DCS dialog box, complete the following field:
    - **HTTPS Certificate**: Select the required certificate from the list. This list corresponds to the logical names in the Keystore, for example, DCSS1-FQDN-Cert.

      ✱ **Note:**

      This certificate must be based on the FQDN, not the IP address.
5. Click **Apply**.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

**Related links**

Deploying and starting the new DCS on page 270

## Starting the new DCS

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Document Conversion Servers** > **Document Conversion Servers**.
2. Select the DCS, for example, **DCS1**.
3. Select **NE Maintenance** from the lefthand menu.
4. On the **Maintenance** dialog, click **Deploy**.

   The Maint state changes from **None** to **Deploying**, indicating that the deploy operation is in progress. When the deploy operation is complete, the Maint state changes back to **None**, and the Admin state changes from **Configured** to **Offline**.
5. Click **Start**.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

**Related links**

Deploying and starting the new DCS on page 270

# Setting up the database replication

In a redundant deployment, a database on the primary side is replicated to the secondary side. This replication process means that the database is copied so that, in the unlikely event of the primary server going offline, Avaya Aura® Conferencing maintains a copy of all conferencing account information.

Previously, you stopped the replication process. Now, in this procedure, you must restart it again, to ensure redundancy functionality on the new system.

## About this task

Use the following procedure to set up database replication.

## Procedure

1. Log on to the server hosting Element Manager instance 0 as `ntappadm` or an account with the AA role.
2. Type `cd /var/mcp/install` and press **Enter**.
3. Type `./setupDBReplication.pl` and press **Enter**.

   The system displays the following information:

   ```
   Deploying files to xxx.xxx.xxx.xxx...
   Deploying files to the Secondary DB
   Deploying files to xxx.xxx.xxx.xxx...
   DB Operation Completed.
   Resync from primary DB to secondary DB.
   This will take a while, please be patient and wait ... setupDBReplication.pl
   completed successfully
   ```

   **Note:**

   If this information is not displayed, stop and contact your next level of support.
4. In the Element Manager Console, verify that the alarms **No connection to DB** instance clear within a couple of minutes.

## Result

The database replication is set up.

## Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

### Related links

Deploying and starting the new DCS on page 270

# Chapter 16: Configuring Document Conversion Servers

## A single document conversion server (DCS) or multiple DCSs?

You can add several Document Conversion Servers (DCSs) to your deployment, depending on your needs and the expected traffic. You can add, modify, and delete DCSs using the Element Manager interface. You can also use the Element Manager interface to start, stop, deploy, and undeploy each DCS instance, as you would any other network element.

The load balancing aspect of the DCS uses the concepts of locations and pools. These are optional configuration settings and are only relevant in a deployment with several DCS servers. You can assign a DCS to a particular location. You can also assign a DCS to a pool of DCSs. In addition, you can assign a particular DCS to be the default DCS for your system. When Avaya Aura® Conferencing chooses which DCS to use for a particular conference, it uses the following process:

- Avaya Aura® Conferencing checks if there is a DCS provisioned to serve the user (conference owner) in their location.
- If there are still no DCS available, Avaya Aura® Conferencing uses the default DCS.
- If there is no location DCS available and no default DCS available, Avaya Aura® Conferencing checks for an available DCS in the pool.

As an aside, the default DCS can be part of the pool of DCSs, but the selection rules still apply.

You can assign DCS instances to particular locations using the Provisioning Client interface. So, the typical order for managing your DCS is that you create and deploy DCS instances using Element Manager. Then you assign the deployed DCSs to particular locations using the Provisioning Client.

## Managing document conversion servers

The document conversion server (DCS) is a Linux® server that converts Microsoft Word, Microsoft PowerPoint, Microsoft Excel, and other document types, such as .PDF and .TXT into a format for content sharing using web conferencing. The DCS also converts graphics, such as .PNG or .JPG images. Avaya Aura® Conferencing hosts the document conversion server as a network element.

Use the procedures in this section to add, modify, and delete a document conversion server.

**Note:**

To upgrade the document conversion server, see *Upgrading Avaya Aura® Conferencing*, which is available from Avaya Support.

**Related links**

Adding a web conferencing document conversion server on page 276
Modifying a web conferencing document conversion server on page 277
Deleting a web conferencing document conversion server on page 281
Configuring the default document conversion server on page 281

## Adding a web conferencing document conversion server

### About this task

Use this procedure to add a web conferencing document conversion server.

### Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Document Conversion Servers > Document Conversion Servers**.
2. In the Document Conversion Servers window, click **Add (+)**.
3. In the Add Document Conversion Server dialog box, complete the fields as appropriate.
4. When finished, click **Apply**.

### Next steps

When you add a new network element, it is likely that you are also changing IP addresses and reconfiguring the NTP, DNS, and Syslog server. If you are making so many changes in your Avaya Aura® Conferencing system, you should always check if the Access Control List (ACL) is applied to the network element. The ACL manages the rules for internal and external system connections. If the ACL is applied to the network element, you should apply it to the new network element. For instructions on checking if it is applied and then applying it, see *Deploying Avaya Aura® Conferencing*, which is available from https://support.avaya.com/. The *Deploying Avaya Aura® Conferencing* guide also describes how to change IP addresses, reconfigure servers, and so on.

**Related links**

Managing document conversion servers on page 275
Add/Edit Document Conversion Server field descriptions on page 276

## Add/Edit Document Conversion Server field descriptions

| Name | Description |
|---|---|
| **ShortName** | A short name to identify the DCS. |

*Table continues…*

| Name | Description |
|---|---|
| **LongName** | A longer, more descriptive name to identify the DCS. |
| **Base Port** | The port that the DCS uses (46000). |
| **FPM** | Displays **Element Manager**. |
| **Access Key** | |
| **HTTPS Certificate** | Choose the FQDN security certificate to be used by this DCS. |
| **DCS Service FQDN** | FQDN for the document conversion server. |

| Button | Description |
|---|---|
| **Apply** | Click **Apply** to save your changes. |
| **Cancel** | Click **Cancel** to clear your changes. |

**Related links**

Adding a web conferencing document conversion server on page 276

## Modifying a web conferencing document conversion server

### About this task

Use this procedure to modify a web conferencing document conversion server.

### Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Document Conversion Servers > Document Conversion Servers**.
2. In the Document Conversion Servers window, select the document conversion server you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Document Conversion Server dialog box, make your changes.
5. When finished, click **Apply**.

**Related links**

Managing document conversion servers on page 275
Modifying the configuration parameters of a document conversion server on page 277
Adding custom fonts on page 280
Add/Edit Document Conversion Server field descriptions on page 276

## Modifying the configuration parameters of a document conversion server

### About this task

Use this procedure to modify the configuration parameters of a document conversion server.

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Document Conversion Servers** > **Document Conversion Servers** > ***<Document Conversion Server name>*** > **Configuration Parameters**.
2. In the Document Conversion Server Configuration Parameters window, make your changes. Use the **Parm Group** drop-down list box to access the parameter(s) you want to modify.

   For more information, see Document Conversion Server Configuration Parameters window field descriptions on page 278.

**Related links**

Modifying a web conferencing document conversion server on page 277
Document Conversion Server Configuration Parameters window field descriptions on page 278

## Document Conversion Server Configuration Parameters window field descriptions

| Parameter group | Configuration parameter | Description |
|---|---|---|
| Dcs | dpi | This parameter specifies the resolution (dots per inch) of converted documents. Avaya recommends using the default settings. This parameter is used for Microsoft Excel, PDF and Microsoft Word document conversions.<br>Default: 120 |
| | pageLimit | This parameter specifies the limit of the number of document pages that can be uploaded to the Document Conversion Server (DCS). The DCS fails if a document with a greater number of pages is uploaded.<br>Default: 300 |
| | png_size_limit | This parameter specifies the maximum file size of shared images in the Portable Network Graphic (PNG) format on the Collaboration Agent interface. If a PNG file is greater than this size, Avaya Aura® Conferencing saves the file as a Joint Photographic Group (JPG) file.<br>Default: 102400 bytes |
| | ppt_height | This parameter specifies the height of Microsoft Powerpoint slides that are displayed on the Collaboration Agent interface.<br>Default: 768 pixels |
| | ppt_width | This parameter specifies the width of Microsoft Powerpoint slides that are displayed on the Collaboration Agent interface. |

*Table continues…*

| Parameter group | Configuration parameter | Description |
|---|---|---|
| | | Default: 1024 pixels |
| TLSAuth | Disable hostname verifier | This parameter enables or disables hostname verification check on certificate validation.<br>Range: true or false<br>Default: false |
| | EnableCRL | This parameter enables CRL retrieval for certificate revocation status.<br>Range: true or false<br>Default: false |
| | EnableOCSP | This parameter enables OCSP retrieval for certificate revocation status.<br>Range: true or false<br>Default: false |
| | EnforceTLSMutualAuthForHTTPS | This parameter enforces TLS Mutual Authentication for HTTP interface.<br>Range: true or false<br>Default: false |
| | PermitNoRevocationValidateResp | This parameter permits access, if no certificate revocation validation response.<br>Range: true or false<br>Default: true |
| Cross-Domain Policy | AllowAccessFromDomains | This parameter specifies the list of domains to which Avaya Aura® Conferencing (AAC) permits access to its Adobe Flash-based features. If a domain is not in this list, the clients in this domain will not be able to access features such as Web Collaboration or the document library. By default, Avaya Aura® Conferencing permits access for any domain. However, if Avaya Aura® Conferencing administrators wish to harden their system, they can limit access, by specifying certain domains and/or IP addresses, with multiple values separated by a comma. |
| WebServer | EnableAccessLogs | This parameter enables Tomcat Access/Error logs.<br>Range: true, false<br>Default: false |

## Related links

Modifying the configuration parameters of a document conversion server on page 277

## Adding custom fonts

By default, Avaya Aura® Conferencing can handle documents with a large variety of fonts. These fonts are:

- Arial Narrow
- Book Antiqua
- Bookman Old Style
- Comic Sans
- Corsiva
- Courier New
- CSongGB18030C-Light
- FBBlueMingL
- Georgia
- Century Gothic
- Impact
- MSung HK Light
- MotoyaExMincho
- Century Schoolbook
- Sorts
- Symbol
- Tahoma
- Times New Roman
- Trebuchet
- Verdana
- Webdings
- Wingdings
- Wingdings 2
- Wingdings 3

If you want your deployment of Avaya Aura® Conferencing to support additional fonts, you must add them. You can also delete any custom fonts. If you choose to add or delete any custom fonts, you must redeploy the Document Conversion Server (DCS) network element.

### About this task

Use this procedure to add custom fonts.

### Procedure

1. Create a zip archive with all of the custom fonts that you want to add.

   Font files must be in TrueType format and placed in the root of the zip archive.
2. In the navigation pane of Element Manager Console, click **Feature Server Elements** > **Document Conversion Servers** > **Custom Fonts**.
3. Click **Browse** to select the zip archive of fonts that you have created.
4. Click **Upload**.
5. Redeploy the Document Conversion Server (DCS) network element.

**Related links**

Modifying a web conferencing document conversion server on page 277

## Deleting a web conferencing document conversion server

In order to fully delete a document conversion server (DCS), you must delete the DCS instance and delete the DCS network element (NE).

### About this task

Use this procedure to delete a web conferencing document conversion server.

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Document Conversion Servers** > **Document Conversion Servers** > ***<DCS name>*** > **Instance**.
2. Click **Delete (-)**.
3. In the Confirmation dialog box, click **Yes**.
4. Navigate to **Feature Server Elements** > **Document Conversion Servers**.
5. In the Document Conversion Servers window, select the document conversion server you want to delete from the list of document conversion servers.
6. Click **Delete (-)**.
7. In the Confirmation dialog box, click **Yes**.

**Related links**

Managing document conversion servers on page 275

## Configuring the default document conversion server

### About this task

Use this procedure to configure a default document conversion server.

### Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Document Conversion Servers > Document Conversion Servers**.
2. Select **Default Document Conversion Server**.
3. From the **Document Conversion Server** drop-down list, select a document conversion server.
4. Click **Apply**.

**Related links**

Managing document conversion servers on page 275

## Managing document conversion server instances

You can also use the Element Manager interface to start, stop, deploy, and undeploy each document conversion server (DCS) instance, as you would any other network element.

**Related links**

Deploying a document conversion server instance on page 282
Undeploying a document conversion server instance on page 283
Starting a document conversion server instance on page 283
Stopping a document conversion server instance on page 283
Restarting a document conversion server instance on page 284
Killing a document conversion server instance on page 284
Modifying a document conversion server instance on page 285

## Deploying a document conversion server instance

### About this task

Use this task to deploy a document conversion server instance.

### Procedure

1. In the navigation pane of Element Manager console, select **Feature Server Elements** > **Document Conversion Servers** > **Document Conversion Servers** > ***<Document conversion server name>*** > **NE Maintenance**.
2. In the Document Conversion Server Maintenance dialog, select the instance that you want to deploy.
3. Click **Deploy**.

**Related links**

Managing document conversion server instances on page 282

## Undeploying a document conversion server instance

### About this task

Use this task to undeploy a document conversion server instance.

### Procedure

1. In the navigation pane of Element Manager console, select **Feature Server Elements** > **Document Conversion Servers** > **Document Conversion Servers** > ***<Document conversion server name>*** > **NE Maintenance**.
2. In the Document Conversion Server Maintenance dialog, select the instance that you want to undeploy.
3. Click **Undeploy**.

**Related links**

Managing document conversion server instances on page 282

## Starting a document conversion server instance

### About this task

Use this task to start a document conversion server instance.

### Procedure

1. In the navigation pane of Element Manager console, select **Feature Server Elements** > **Document Conversion Servers** > **Document Conversion Servers** > ***<Document conversion server name>*** > **NE Maintenance**.
2. In the Document Conversion Server Maintenance dialog, select the instance that you want to start.
3. Click **Start**.

**Related links**

Managing document conversion server instances on page 282

## Stopping a document conversion server instance

### About this task

Use this task to stop a document conversion server instance.

### Procedure

1. In the navigation pane of Element Manager console, select **Feature Server Elements** > **Document Conversion Servers** > **Document Conversion Servers** > ***<Document conversion server name>*** > **NE Maintenance**.
2. In the Document Conversion Server Maintenance dialog, select the instance that you want to stop.
3. Click **Stop**.

**Related links**

Managing document conversion server instances on page 282

## Restarting a document conversion server instance

### About this task

Use this task to restart a document conversion server instance.

### Procedure

1. In the navigation pane of Element Manager console, select **Feature Server Elements** > **Document Conversion Servers** > **Document Conversion Servers** > ***<Document conversion server name>*** > **NE Maintenance**.
2. In the Document Conversion Server Maintenance dialog, select the instance that you want to restart.
3. Click **Restart**.

**Related links**

Managing document conversion server instances on page 282

## Killing a document conversion server instance

### About this task

Use this task to kill a document conversion server instance.

### Procedure

1. In the navigation pane of Element Manager console, select **Feature Server Elements** > **Document Conversion Servers** > **Document Conversion Servers** > ***<Document conversion server name>*** > **NE Maintenance**.
2. In the Document Conversion Server Maintenance dialog, select the instance that you want to kill.
3. Click **Kill**.

**Related links**

Managing document conversion server instances on page 282

## Modifying a document conversion server instance

### About this task

Use this procedure to modify a document conversion server instance.

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Document Conversion Servers** > **Document Conversion Servers** > ***<Document Conversion Server name>*** > **Instance**.
2. In the Document Conversion Server Instance window, select the server instance you want to modify.
3. Click **Edit (-/+)**.
4. In the Edit Document Conversion Server Instance dialog box, make your changes. To change the Eng Parms, click **Advanced**.
5. When finished, click **Apply**.

### Example

This document does not contain an exhaustive description of each engineering parameter. Avaya recommends maintaining the parameter default values. For reference only, the following table describes the Dcs engineering parameters.

| Parameter name | Value |
|---|---|
| DcsMaxTuples | This parameter specifies the maximum number of tuples that the DCS in memory database table can have.<br>The default settings are:<br>• For a small deployment: 1000<br>• For a medium deployment: 1500<br>• For a large deployment: 2000 |
| graceful_shutdown_time | This parameter specifies the time allowed for the DCS to gracefully shutdown all running jobs (if any) before coming to a stop.<br>The default setting is 5 seconds. |
| max_active_jobs | This parameter specifies the number of threads assigned to the DCS for conversion. The default settings is 4. This value is required for a large |

*Table continues…*

| Parameter name | Value |
|---|---|
| | configuration but should be configured to 2 or 1 for a medium or small configuration.<br>The default settings are:<br>• For a small deployment: 1<br>• For a medium deployment: 2<br>• For a large deployment: 4 |
| max_job_time | This parameter specifies the maximum time allowed by the DCS for a given conversion before it times out.<br>The default setting is 1200000 seconds (20 minutes). |
| max_jobs | This parameter specifies the maximum number of active jobs that can run at any point in time.<br>The default setting is 25. |
| upload_max_filesize | This parameter specifies the maximum upload file size allowed for conversion by the DCS.<br>The default setting is 30720000 bytes (30Mb)<br>**Note:**<br>This parameter does not apply to image uploads. For image uploads, for both PNG and JPG formats, the maximum file size limit is 12 Mb and the maximum resolution allowed is 23 mega pixels in total. This is not configurable through the DCS. |

**Note:**

All changes to the Engineering Parameters require a restart.

**Related links**

Managing document conversion server instances on page 282

# Assigning document conversion servers to locations

For the purposes of load balancing, you must assign document conversion servers (DCSs) to locations. This way, you can insure that server selection is based on load performance factor and that Avaya Aura® Conferencing always distributes conversion requests in such a way as to minimize the conversion time.

You can assign a DCS to a location using the Provisioning Client. This functionality is located in the WCS Clusters section of the Provisioning Client. For more information, see:

- Assigning WCS clusters to serving locations on page 252
- WCS cluster/DCS serving locations tab field descriptions on page 252

# Adding additional DCS hosts

### Before you begin

Install the Avaya Aura® Conferencing software on a server.

For more information, see Installing Avaya Aura Conferencing on page 121.

### About this task

Use this procedure if you want to add expansion DCSs.

### Procedure

1. In the navigation pane of Element Manager Console, click **Addresses**.
2. In the Addresses window, click **Add (+)**.
3. In the Add IPv4 Address dialog box, enter the logical name and IP address for the server on which the Document Conversion Server software will be installed.
4. Click **Apply**.
5. In the navigation pane of Element Manager Console, click **Servers**.
6. In the Servers window, click **Add (+)**.
7. In the Add Server dialog box, complete the following fields:
   - **Short Name**
   - **Long Server Name**
   - **Physical site**
   - **Internal OAM (Default) Address**: Enter the IP address you specified in Step 3.
   - **Operating System**: Select **linux**.
8. Click **Apply**.

### Next steps

Proceed to Adding an Avaya Aura Media Server network element on page 243.

# Chapter 17: Deploying and starting the remaining Network Elements

## Starting Server Monitors

### About this task

The monitor service reports the following critical resource information about the server:

- CPU usage
- physical memory usage
- network I/O usage
- file system disk usage

Use this procedure to start the monitor service for each server in your configuration.

### Procedure

1. In the navigation pane of Element Manager Console, click **Servers > <*Server name*> > Monitor**.
2. In the Server Monitor window, click **Start Monitor**.

   The following message appears at the bottom of the window: “The server monitor is running.”
3. Wait for the RAM, Disk, CPU, and Interface areas to become populated with data.

   **Note:**

   It is normal for alarms to be raised and then cleared as the system initializes. If any server monitoring alarms are not cleared, contact the Avaya support Web site at http://support.avaya.com to open a service request.
4. Repeat steps 1 through 3 for every server displayed in the Servers folder in Element Manager Console.

### Next steps

Start the database monitors.

# Starting Database Monitors

### About this task

The monitor service reports the data replication status for the mcpdb database.

### Procedure

1. In the navigation pane of the Element Manager Console, click **Feature Server Elements > Database > mcpdb > Monitor**.
2. In the mcpdb Monitor window, click the row containing **0** in the Instance Number column.
3. Click **Monitor**.

   The mcpdb_0 Database Instance Monitor window appears.
4. Click **Start Monitor**.

   The message `database instance monitor is running` appears at the bottom of the window.
5. Wait for the General Information and Database Process Status areas to update.

   **Note:**

   It is normal for alarms to be raised and then cleared as the system initializes. If any monitoring alarms are not cleared, contact the Avaya support Web site at http://support.avaya.com to open a service request.
6. Close the mcpdb _0 Database Instance Monitor window.
7. Repeat steps 2 through 6 for instance number 1 (if configured).
8. When finished, close the mcpdb Monitor window.

# Deploying and starting secondary Element Manager Network Element

Element Manager is a component of Element Manager Console that manages all the network elements. For Avaya Aura® Conferencing to be operational, the Element Manager must be deployed and started.

**Note:**

If the Element Manager is not running, logs and alarms are spooled but conferencing services are available.

### About this task

Use the following procedure to start and deploy Element Manager instance 1 for SMB and medium deployments with redundancy and large deployments with redundancy. If you have an

SMB/medium simplex or a large simplex deployment type, you can skip this procedure and proceed to deploying and starting an Accounting Manager Network Element.

### Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Element Manager > Element Manager > NE Maintenance**.
2. In the Element Manager Maintenance dialog box, select the row for ID 1.
3. Click **Deploy**.

   The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.
4. Click **Start**.

   The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

   Check the state transitions for the following fields:

| Field | Status |
|---|---|
| Maint | None |
| Admin | Online |
| Link | Up |
| Oper | Active or Hot Standby |

### Next steps

Deploy and start the accounting manager network elements.

## Deploying and starting an Accounting Manager Network Element

Accounting Manager is a component of Element Manager Console that manages all the billing and accounting details.

### About this task

Use the following procedure to deploy and start an Accounting Manager instance.

### Procedure

1. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Accounting Managers** > **AM1** > **NE Maintenance**.
2. In the Accounting Manager Maintenance dialog box, select the row for ID 0.

3. Click **Deploy**.

   The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.

4. Click **Start**.

   The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

   Check the state transitions for the following fields:

   | Field | Status |
   |---|---|
   | Maint | None |
   | Admin | Online |
   | Link | Up |
   | Oper | Active or Hot Standby |

5. In the Accounting Manager Maintenance dialog box, select the row for ID 1, for non-simplex deployments.

   **Note:**

   If you have a simplex deployment type, skip the remaining steps and proceed to deploying and starting a Provisioning Manager Network Element.

6. Click **Deploy**.

   The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.

7. Click **Start**.

   The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

   Check the state transitions for the following fields:

   | Field | Status |
   |---|---|
   | Maint | None |
   | Admin | Online |
   | Link | Up |
   | Oper | Active or Hot Standby |

## Next steps

Deploy and start the Provisioning Manager Network Elements.

# Deploying and starting a Provisioning Manager Network Element

Provisioning Manager is a component of the Element Manager Console that manages configurational procedures.

### About this task

Use the following procedure to deploy and start a Provisioning Manager instance.

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Provisioning Managers** > <*Provisioning Manager name*> > **NE Maintenance** .

   Where *Provisioning Manager name* is Prov1.

2. In the Prov1 NE Maintenance dialog box, select the row for ID 0.

3. Click **Deploy**.

   The dialog box displays the status of the following fields:

   | Field | Status |
   |---|---|
   | Admin | Offline |
   | Link | Down |
   | Oper | Unavailable |

4. Click **Start**.

   The dialog box displays the updated status of the following fields:

   | Field | Status |
   |---|---|
   | Admin | Online |
   | Link | Up |
   | Oper | Active |

5. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Provisioning Managers** > <*Provisioning Manager name*> > **NE Maintenance** .

   Where *Provisioning Manager name* is Prov2.

6. In the Prov2 NE Maintenance dialog box, select the row for ID 0.

7. Click **Deploy**.

   The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.

8. Click **Start**.

The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

Check the state transitions for the following fields:

| Field | Status |
|---|---|
| Maint | None |
| Admin | Online |
| Link | Up |
| Oper | Active |

### Next steps

Proceed to deploying and starting an Application Server Network Element.

## Deploying and starting an Application Server Network Element

For (SMB, medium, and large) redundant configurations, you can configure failover capability.

### About this task

Use the following procedure to deploy and start an Application Server Network Element.

### Procedure

1. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Application Servers** > **AS1** > **NE Maintenance**.
2. In the Application Server Maintenance dialog box, select the row for ID 0.
3. Click **Deploy**.

   The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.
4. Click **Start**.

   The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

   Check the state transitions for the following fields:

| Field | Status |
|---|---|
| Maint | None |

*Table continues…*

| Field | Status |
|---|---|
| Admin | Online |
| Link | Up |
| Oper | Active or Hot Standby |

5. In the Application Server Maintenance dialog box, select the row for ID 1.

   **Note:**

   If you have a simplex deployment, you can skip steps 5 through 7.

6. Click **Deploy**.

   The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.

7. Click **Start**.

   The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

   Check the state transitions for the following fields:

| Field | Status |
|---|---|
| Maint | None |
| Admin | Online |
| Link | Up |
| Oper | Active or Hot Standby |

### Next steps

Proceed to enabling replication on the Avaya Aura® Media Server if you have two or more Avaya Aura® Media Servers in one Media Server cluster.

## Enabling replication on the Avaya Aura® Media Server

If you have two or more Avaya Aura® Media Servers in one Media Server cluster, you must enable replication.

### About this task

Use the following procedure to enable replication on the Avaya Aura® Media Server.

### Procedure

1. On the Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Server Clusters** > *<Media Server cluster name>*.

2. Click **Replication Settings**.
3. In the Replication Settings dialog box, complete the following fields:
    - **Enable Replication Account**: Select the check box.
    - **User Name**: Type the User Name. Must be 6 to 8 characters in length.
    - **Password**: Type a password. Use the password rules as defined for Element Manager.
    - **Confirm**: Type the password again to confirm.
4. Click **Apply**.

### Next steps

Proceed to Deploying and starting the Avaya Aura® Media Server Network Element.

## Deploying and starting the Avaya Aura® Media Server Network Element

Each Avaya Aura® Media Server instance must be started for the instance and the cluster to which it is attached to be functional.

### About this task

Use the following procedure to deploy and start an Avaya Aura® Media Server Network Element instance.

### Procedure

1. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers** > <*Media Server name*> >**NE Maintenance**.
2. In the Media Server Maintenance dialog box, select the row for ID 0.
3. Click **Deploy**.

    The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.
4. Click **Start**.

    The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

    Check the state transitions for the following fields:

| Field | Status |
|---|---|
| Maint | None |
| Admin | Online |
| Link | Up |
| Oper | Active |

5. Repeat steps 2 through 4 for each additional Avaya Aura® Media Server.

### Result

The deployment of Avaya Aura® Media Server Network Element is complete.

### Next steps

Proceed to Deploying and starting the Web Conferencing Network Elements.

## Deploying and starting the Web conferencing Network Elements

### About this task

Use the following procedure to deploy and start the Web conferencing Network Elements.

### Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Web Conferencing > Web Conferencing Servers and Clusters > Web Conferencing Servers > <*Web conferencing server name*> > NE Maintenance**.
2. In the Web Conferencing Server Maintenance dialog box, select the row for ID 0.
3. Click **Deploy**.

   The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.
4. Click **Start**.

   The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

   Check the state transitions for the following fields:

| Field | Status |
|---|---|
| Maint | None |
| Admin | Online |

*Table continues…*

| Field | Status |
|---|---|
| Link | Up |
| Oper | Active |

### Next steps

Proceed to Deploying and starting the Web Conferencing Management Network Elements.

## Deploying and starting the Web conferencing management Network Elements

### About this task

Use the following procedure to deploy and start the Web Conferencing Management Server network elements.

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Management** > **Web Conferencing Management Servers** > <*Web conferencing management server name*> > **NE Maintenance**.
2. In the Web Conferencing Management Server Maintenance dialog box, select the row for ID 0.
3. Click **Deploy**.

   The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.
4. Click **Start**.

   The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

   Check the state transitions for the following fields:

| Field | Status |
|---|---|
| Maint | None |
| Admin | Online |
| Link | Up |
| Oper | Active |

# Deploying and starting Collaboration Agent Network Elements

## About this task

Use the following procedure to deploy and start the Collaboration Agent Network Elements.

**Note:**

If you have an SMB or medium deployment, you can skip this procedure.

## Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Collaboration Agent Managers** > < *name*> > **NE Maintenance**.
2. In the CA1 NE maintenance dialog box, select the row for ID 0.
3. Click **Deploy**.

   The dialog box displays the status of the following fields:

   | Field | Status |
   |---|---|
   | Admin | Offline |
   | Link | Down |
   | Oper | Unavailable |

4. Click **Start**.

   The dialog box displays the updated status of the following fields:

   | Field | Status |
   |---|---|
   | Admin | Online |
   | Link | Up |
   | Oper | Active |

   **Note:**

   If you have an SMB or medium simplex deployment, skip the remaining steps.

5. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Collaboration Agent Managers** > **CA2**.
6. In the CA2 NE Maintenance dialog box, select the row for ID 0.
7. Click **Deploy**.

   The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.

8. Click **Start**.

The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

Check the state transitions for the following fields:

| Field | Status |
|---|---|
| Maint | None |
| Admin | Online |
| Link | Up |
| Oper | Active |

### Next steps

Proceed to verifying local access to the Provisioning Client.

## Verifying local/emergency access to the Provisioning Client

Administrators usually log on to Provisioning Client through System Manager using single sign-on (SSO). However, in situations where single sign-on is not available, such as a network issue, you can use local/emergency access.

### Before you begin

You must know the following:

- The IP address of EMServer1
- The IP address of EMServer2: for redundant deployments only
- The FQDN of the Provisioning Server

⚠ **Warning:**

During local/emergency access, the administrator must be aware of the following:

- Additional expert mode privileges are granted which allow you to directly modify data which is usually controlled by System Manager.
- Where the expert mode warning appears, any changes made to these pages can cause synchronization issues between System Manager and Provisioning Client.

### About this task

Use this procedure to verify local/emergency access to the Provisioning Client for Avaya Aura® Conferencing on EMServer1 and EMServer2.

### Procedure

1. On your PC, open the browser.
2. In the Address box, enter the following address:

```
https://<FQDN>:8443/prov
```

where *<FQDN>* is the FQDN of EMServer1.

3. Press **Enter**.
4. Click **Continue to this website**.

   The Provisioning Client Login window appears.

   > **Note:**
   >
   > If the Provisioning Client page does not appear, contact the Avaya support Web site at http://support.avaya.com to open a service request.

5. In the Username box on the Provisioning Client Login window, enter `admin`.
6. In the Password box, enter `admin`.
7. Click **Login**.

   The Welcome to the Provisioning Client page appears.

8. Click Logout.

   Complete the following steps if your deployment model supports a secondary Provisioning Manager.

9. In the Address box of the Web browser, enter the following address:

   ```
   https://<FQDN>:8443/prov
   ```

   where *<FQDN>* is the FQDN of EMServer2.

10. Press **Enter**.
11. Click **Continue to this website**.

    The Provisioning Client Login window appears.

12. In the Username box on the Provisioning Client Login window, enter `admin`.
13. In the Password box, enter `admin`.
14. Click **Login**.

    The Welcome to the Provisioning Client page appears.

15. Click **Logout**.

### Next steps

Verify local access to Collaboration Agent.

## Verifying local access to Collaboration Agent

## Before you begin

You must know the IP address of:

- EMServer1
- EMServer2: for redundant deployments only

## About this task

Use this procedure to verify that you can access the Collaboration Agent Login window locally on EMServer1 and EMServer2.

**Important:**

You must provision at least one System Manager domain on the Avaya Aura® Conferencing system before you can access the Collaboration Agent.

## Procedure

1. On your PC, open the browser.
2. In the Address field, enter the following address:

   ```
   https://<FQDN>/aacpa
   ```

   where *<FQDN>* is the FQDN of EMServer1.
3. Press **Enter**.

   The Avaya Aura® Conferencing Collaboration Agent Login window appears.

   **Note:**

   If the Avaya Aura® Conferencing Collaboration Agent Login window does not appear, contact the Avaya support Web site at http://support.avaya.com to open a service request.
4. Close the Avaya Aura® Conferencing Collaboration Agent Login window.
5. In the Address field of the Web browser, enter the following address:

   ```
   https://<FQDN>/aacpa
   ```

   where *<FQDN>* is the FQDN of EMServer2.
6. Press **Enter**.

   The Avaya Aura® Conferencing Collaboration Agent Login window appears.
7. If you have a large simplex deployment, in the Address field of the Web browser complete the following or skip to the next step.

   ```
   https://<FQDN>/aacpa
   ```

   where *<FQDN>* is the FQDN of PA1.
8. Press **Enter**.

   The Avaya Aura® Conferencing Collaboration Agent Login window appears.

9. If you have a large deployment with redundancy, in the Address field of the Web browser complete the following:

   `https://<FQDN>/aacpa`

   where *<FQDN>* is the FQDN of PA2.
10. Press **Enter**.

    The Avaya Aura® Conferencing Collaboration Agent Login window appears.

### Next steps

Verify the status of all system components.

## Verifying the status of all system components

### About this task

Use this procedure to verify:

- all components are running
- there are no alarms present

### Procedure

1. On the management PC, open the browser.
2. In the Address box, enter the following address:`https://<FDQN>:12121`

   where *<FQDN>* is the Element Manager FQDN. (This is the server running Element Manager Console.)
3. Press **Enter**.

   A Web page appears displaying the FQDN you entered and the link **Launch Element Manager Console**.
4. Click **Launch Element Manager Console**.
5. From the IPv4 Service Address box on the Element Manager Console window, select the FQDN of the server running Element Manager console.
6. Click **Connect**.

   A connection is established to the active element manager (EM) instance.
7. In the UserID box on the Element Manager Console window, enter `admin`.
8. In the Current Password box, enter `admin`.
9. Click **Ok**.

   The Element Manager Console window appears.

10. Look at the alarm bar at the top of the window and verify the following items:
    - The alarm bar is green.
    - The Total Alarms, Critical, Major, Minor, and Warning fields display **0**.

    **Note:**

    If the alarm bar is not green, and there are alarms, contact the Avaya support Web site at http://support.avaya.com to open a service request.
11. Right-click the mouse on the alarm bar, and select **Logical View**.
12. In the Logical View window, expand each folder, and verify that component has a green icon preceding it.

    **Note:**

    If all of the folder components do not have a green icon, contact the Avaya support Web site at http://support.avaya.com to open a service request.
13. When finished, close the Logical View window.

# Chapter 18: Configuring single sign-on for Element Manager Console and Provisioning Client

## Introduction

System Manager is a central management system that delivers a set of shared management services and a common console across multiple products. With single sign-on (SSO) enabled for Avaya Aura® Conferencing, you can administer all the components using System Manager. This chapter provides the procedures to configure SSO, configure System Manager to recognize each network element, and configure the administrator PC.

## Configuring time on System Manager and network elements

### About this task

To use single sign-on (SSO), System Manager and all the network elements must have synchronized clocks. A clock skew of a few seconds results in SSO to fail. If the Home portlet is missing menus or functions, logon access to the Element Manager Console or Provisioning Client can fail.

**Note:**

Ensure your servers use the Network Time Protocol (NTP) time sources.

### Procedure

1. Log on to the System Platform Console.
2. In the navigation pane, click **Server Management** > **Date/Time Configuration**.
3. On the Server Management Date/Time Configuration page, verify that you are using NTP server in the Manage Time Servers area. If only **Local Clock** displays, add at least one NTP server and in the Added Servers field, and click **start ntpd**. Use the **Primary Clock Source** and **Secondary Clock Source** values, and check the **Local Time** value.

> **Warning:**
>
> Clicking start ntpd causes the system platform and server to restart.

4. Open an SSH connection and log into EMServer1 as `ntsysadm` to verify the time on the server.
5. Type `date`, and press **Enter**.
6. Compare the time on the System Platform Console with the time on the application server. If the time difference between the System Platform Console and the application server is greater than 60 seconds, perform the following steps:
    a. Verify that the NTP is configured on the application server.
    b. On the application server, run the ntpConfig tool.
    c. Type `c` to configure.
    d. Use the **Primary Clock Source** and **Secondary Clock Source** values
    e. Type `date`, and press **Enter**.
    f. Compare the time on the System Platform console with the time on EMServer1. If the time difference between the System Platform Console and the application server is still greater than 60 seconds, perform Steps G through K to correct the date and time manually on the application server by forcing the NTP time update.
    g. At the command prompt, enter `su –` to log in as root.
    h. After you log in as root, type `service ntpd stop`, and press **Enter** to stop the ntpd service.
    i. Run `/usr/sbin/ntpdate <Primary Clock Source IP address>` to update the system time.
    j. Type `date`, and press **Enter** to verify that the date and time have been adjusted.
    k. Type `service ntpd start`, and press **Enter** to start the ntpd service.
7. Repeat Steps 5 and 6 for each application server.

### Next steps

Proceed to configuring network element FQDNs in System Manager.

## Configuring the application server network elements on System Manager

### About this task

Details of each Network Element must be added in the System Manager inventory so that it is possible to launch the Network Elements directly from System Manager. To configure details of each Element Manager, use the following procedure.

**Note:**

System Manager must have only PROVs from one Avaya Aura® Conferencing system in your inventory. If you have another Avaya Aura® Conferencing system, and you enter the PROV elements in the System Manager inventory, you can encounter problems. System Manager always sends conferencing profile data to one PROV. The data is sent to the first available PROV in the inventory.

**Note:**

To use single sign-on (SSO), the System Manager FQDN, Element Manager FQDN, and Provisioning Client FQDN (if required) must belong to the same root domain.

### Procedure

1. Log on to System Manager as admin.
2. On the System Manager console, click **Inventory**.
3. In the navigation pane, click **Manage Elements**.
4. On the Manage Elements page, click **New**.
5. In the **General** section on the New Elements page, select **Conferencing** from the **Type** list.

   The page refreshes and additional fields appear.
6. In the **General** section on the New Conferencing page, complete the following fields:
   - **Name**: Type `AAC-EM`.
   - **Node**: Type the FQDN of the Element Manager Service IP address.
7. Click **Access Point**.
8. In the Access Point section, click **New**.
9. In the Access Point Details section, complete the following fields:
   - **Name**: Type the FQDN of the Element Manager Service IP address.
   - **Access Point Type**: Select **EMURL**.
   - **Protocol**: Select **https**.
   - **Host**: Type the FQDN of the Element Manager Service IP address.
   - **Port**: Type `12121`.
   - **Path**: Type `sso`.
   - **Order**: Type `0`.
10. Click **Save**.
11. Click **Commit**.

    The addition of Element Manager on System Manager is now complete.

12. For Provisioning Manager, perform the following steps:
    a. On the Manage Elements page, click **New**.
    b. On the New Elements page, complete the following fields:
       - **Name**: Type `AAC-PROV`.
       - **Type**: Select **Conferencing**.
       - **Node**: Type the FQDN of the EMServer1.
    c. Click **Access Point**.
    d. In the Access Point area, click **New**.
    e. In the Access Point Details area, complete the following details:
       - **Name**: Type the IP address of EMServer1.
       - **Access Point Type**: Select **EMURL**.
       - **Protocol**: Select **https**.
       - **Host**: Type the FQDN of the EMServer1.
       - **Port**: Type `8443`.
       - **Path**: Type `prov/sso`.
       - **Order**: Type `0`.
    f. Click **Save**.
    g. Click **Commit**.

       The addition of Provisioning Client on System Manager is now complete.

### Next steps

Proceed to Launching Element Manager Console and Provisioning Client from System Manager.

## Launching Element Manager Console and Provisioning client from System Manager

After single sign-on is enabled, you can launch network elements directly from System Manager.

**Note:**

System Manager administrators have permissions for controlling access to Conferencing and Element Manager and Provisioning Client elements. By default, administrators with either Network Administrator or System Administrator roles have read, write, and expert mode permissions. You can change role assignments and configure permissions for access to various elements. On System Manager home page, click **Users** > **Administrators**.

⚠ **Warning:**

If you have Expert mode privileges, you see an Expert mode warning on certain Provisioning Client pages. This mean that the data on this page is normally controlled by System Manager. Only make changes on these pages to fix synchronization issues with System Manager.

### About this task

Use the following procedure to launch the Element Manager Console and Provisioning Client from System Manager.

### Procedure

1. Log on to System Manager.
2. On the System Manager console, click **Elements** > **Conferencing**.
3. On the Conferencing Dashboard page, in the **Name** column, select the name of Element Manager Console.
4. From the IPv4 Service Address box on the Element Manager Console window, select the IP address of the server running Element Manager Console.
5. Click **Connect**.

   The Element Manager Console window appears.
6. From the Element Manager Console menu bar, select **File** > **Exit** to exit Element Manager Console.
7. On the Conferencing Dashboard page, in the **Name** column, select the name of the Provisioning Client you want to access.

   The Welcome to the Provisioning Client page appears.
8. On the Provisioning Client page, click **Logout**.

### Result

The Element Manager Console and Provisioning client can now be launched from System Manager.

# Chapter 19: Configuring routing between System Manager and Avaya Aura® Conferencing

## Configuring the route to Avaya Aura® Conferencing on System Manager

### About this task

Use the following procedure to configure the route to Avaya Aura® Conferencing from System Manager.

### Procedure

1. Log in to System Manager.
2. On the System Manager console, click **Elements** > **Routing**.
3. In the navigation pane, click **SIP Entities**.
4. On the SIP Entities page, click **New**.
5. Complete the following fields:
    - **Name**: Enter a unique name from 3 to 64 characters for this SIP entity.
    - **FQDN or IP Address**: Type the FQDN or IP address of the AS1 signaling service.
    - **Type**: Select **Conferencing**.

      The screen refreshes to display the following:
    - **Adaptation**: Select from the list.
    - **Location**: Select your location.
    - **Time Zone**: Select a time zone from the list.
    - **SIP Timer B/F (in seconds)**: Type a value between 1 to 32, default is 4.
    - **Credential name**: Type a name.
    - **Call Detail Recording**: Select from the list.
    - **SIP Link Monitoring**: Select **Use Session Manager Configuration**.
    - **Supports Call Admission Control**: Select the check box to enable it.

- **Shared Bandwidth Manager**: Select the check box to enable it.
- **Primary Session Manager Bandwidth Association**: Select your Session Manager entity.
- **Backup Session Manager Bandwidth Association**
- **Override Port & Transport with DNS SRV**: Select the check box to enable it.

6. Click **Commit**.
7. In the navigation pane, click **Entity Links**.
8. On the Entity Links page, click **New**.
9. Complete the following fields:
   - **Name**: Enter a name for this link.
   - **SIP Entity 1**: Select the Aura Session Manager entity.
   - **Protocol**: Select **TCP**.

     **OR**

     Select **TLS**.

     ✱ **Note:**

     If you selected TLS, you must assign a certificate for the Application Server, see Next steps for implementing security on page 555.
   - **Port**: Enter `5060` for TCP or `5061` for TLS.
   - **SIP Entity 2**: Select the Avaya Aura® Conferencing SIP entity you previously created.
   - **Port**: Enter `5060` for TCP or `5061` for TLS.
   - **Connection Policy**: Select **Trusted**.

   ✱ **Note:**

   If TLS is selected for SIP Entity 1 then it must also be selected for SIP Entity 2.
10. Click **Commit**.
11. In the navigation pane, click **Routing Policies**.
12. On the Routing Policies page, click **New**.
13. In the Name box on the Routing Policies page, enter a name for this routing policy.
14. In the SIP Entity as Destination area, click **Select**.
15. On the SIP Entity List page, select the Avaya Aura® Conferencing SIP entity.
16. Click **Select**.
17. Click **Commit**.
18. In the navigation pane, click **Dial Patterns**.

19. On the Dial Patterns page, click **New**.
20. In the Pattern box on the Dial Pattern Details page, type the routing/pilot number that is part of the dialing number to join MeetMe conferences.
21. In the Min box, type the number of digits that match the pattern number. This is the minimum number of digits in the dialing number.
22. In the Max box, type the number of digits that match the pattern number. This is the maximum number of digits in the dialing number.
23. In the Originating Location and Routing Policies area, click **Add**.
24. In the Originating Location area, select your location.
25. In the Routing Policies area, select the routing policy that you previously created for Avaya Aura® Conferencing.
26. Click **Select**.
27. Click **Commit**.

### Result

You have configured the routing policy so that when you dial a number that contains the pattern you specified, your call goes to the Avaya Aura® Conferencing Application Server.

### Next steps

Proceed to configuring the TLS route to Session Manager from the Element Manager, if TLS is configured; otherwise, proceed to the next chapter.

#### Related links

Making Avaya Aura Conferencing aware of System Manager domains on page 320

## Configuring TLS route to Session Manager from the Element Manager

### Before you begin

You have configured TLS in the previous procedure.

### About this task

Use the following procedure to configure the Application Server route to the Session Manager to use TLS.

### Procedure

1. Log on to System Manager.
2. On the System Manager page, click **Elements** > **Conferencing**.
3. On the Conferencing Dashboard page, in the Name column, select the name of Element Manager Console.

4. Click **Connect**.
5. In the navigation pane of Element Manager Console, click **Avaya Aura Core** > **Session Manager**.
6. In the Session Manager window, select the Session Manager to configure.
7. Click **Edit (-/+).**
8. In the Edit Session Manager dialog box, in the **Enable SIP TLS Port** field, select the check box to enable TLS and verify that the SIP TLS Port is the same as what is configured on the System Manager in the procedure for Configuring the route to Avaya Aura Conferencing on System Manager on page 309.
9. Close the Session Manager window.
10. On the **File** menu, click **Exit** to exit Element Manager Console.

# Chapter 20: Provisioning system settings and users for Avaya Aura® Conferencing

## Adding conference access numbers in Provisioning Client

Within Avaya Aura® Conferencing, conference access numbers are called Service URIs. Service URI is the dialing access number for participants to join an Avaya Aura® Conferencing MeetMe conference. The Service URI number matches the routing dial pattern that you previously configured on the Dial Pattern Details page in Configuring the route to Avaya Aura Conferencing on System Manager on page 309. The Service URI is the user name part of the SIP URI string.

These conference access numbers are displayed to end users on the Collaboration Agent interface and in the Avaya Aura® Conference Manager Add-in for Microsoft Outlook® notification e-mails. However, you can configure alternative display numbers to be displayed to end-users on the Collaboration Agent interface and in the Avaya Aura® Conference Manager Add-in for Microsoft Outlook® notification e-mails.

### About this task

Use the following procedure to add a conference URI.

### Procedure

1. Log in to System Manager.
2. On the System Manager console, click **Elements** > **Conferencing**.
3. In the Name column on the Conferencing Dashboard, click the Provisioning Client.

   A new browser window appears and displays the Avaya Aura® Provisioning Client.
4. In the Provisioning Client window, select **System Management > Routing > Service URI**.
5. On the Service URI tab, complete the following for a MeetMe conference:

   This number must match the routing pattern that you previously configured in System Manager.

   - **Service URI**: Type an access number for a MeetMe conference.
   - **Locale**: Select a location from the list. The locale specifies the default locale of prompts that are used if your SIP client does not provide your locale.

- **Conference Type**: Select **MeetMe** from the list.

6. Click **Save**.
7. On the Service URI tab, complete the following for an Adhoc conference:

   This number must match the routing pattern that you configured in System Manager.

   - **Service URI**: Type an access number for an Adhoc conference.
   - **Locale**: Select a location from the list. The locale specifies the default locale of prompts that are used if your SIP client does not provide your locale.
   - **Conference Type**: Select **Adhoc** from the list.
8. Click **Save**.
9. On the Service URI tab, complete the following for an Event conference:

   This number must match the routing pattern that you previously configured in System Manager.

   - **Service URI**: Type an access number for an Event conference. This number must match the routing pattern that you configured in System Manager.
   - **Locale**: Select a location from the list. The locale specifies the default locale of prompts that are used if your SIP client does not provide your locale.
   - **Conference Type**: Select **Event** from the list.
10. Click **Save**.
11. Repeat Steps 5 through 10 to add additional conference access numbers.

### Next steps

Configure display numbers in Provisioning Client.

**Related links**

Configuring display numbers in Provisioning Client on page 317
Deploying the Avaya Aura Conference Manager Add-in for Microsoft Outlook on page 622

## Creating a user template

### About this task

Use the following procedure to create a new user with predefined settings.

### Procedure

1. Log on to System Manager as admin.
2. On the System Manager console, click **Elements** > **Conferencing**.
3. In the Name column on the Conferencing Dashboard, click Provisioning Client

4. In the Provisioning Client window, select **User Management** > **User Template**.
5. Complete the following:
   - **Name**: Type the name of User Template being created.
   - **Conference class of service**: Select the conference class of service from the list.
   - **Enable Video**: Select the check box to enable video for a particular user of the Multimedia Conferencing service.
   - **Priority**: Select a priority from the list.

   **Note:**

   The priority is determined by the quality of service required for this user. For example, the higher the priority setting, the better the service. The default value is medium.
6. Click **Save**.

## Creating a conference class of service user template

A conference class of service defines configuration details of a user conference. Class of service templates define the video class of service, the number of conference participants, and whether dial out is allowed for a particular group of users who have that template assigned. Avaya Aura® Conferencing provides the following preconfigured conference classes of service that cannot be deleted or modified:

**Table 22: Default conference classes of service**

| Name | Video Class of Service | Allow dial out/Adhoc | Maximum users |
|---|---|---|---|
| executive | ultra_hi_bandwidth_d | yes | 300 |
| desktop_user | hi_bandwidth_d | yes | 50 |
| mobile_high | medium_bandwidth_c | yes | 50 |
| mobile_low | low_bandwidth_c | yes | 50 |
| guest_user | none | no | 10 |

**Note:**

You can skip this procedure if you want to use one of default conference classes of service

### About this task

Use the following procedure to create a conference class of service user template.

### Procedure

1. Log on to System Manager as admin.
2. On the System Manager console, click **Elements** > **Conferencing**.

3. In the Name column on the Conferencing Dashboard, click the Provisioning Client.
4. In the Provisioning Client window, select **System Management** > **Conference Class of Service**.
5. Complete the following fields:
    - **Name**: Type the name of Conference Class being created.
    - **Maximum number of participants**: Type a value between 1 and 3,000 to indicate the allowed number of participants on a chairperson bridge.
    - **Event Conference**: Select this check box if you are creating a large event conference.
    - **Allow dial out to participants**: Select this check box to allow the chairperson to invite participants to the conference.
    - **Conference Flow**: Select conference flow from the list.
    - **Video class**: Select a video class from the list. The parameters for each video class are shown in the table on the window.
6. Click **Save**.

### Next steps

Proceed to creating a video class of service user template.

## Creating a video class of service user template

A video class of service defines the video settings for a user conference.

**Note:**

You can skip this procedure if you want to use one of the default video classes.

### About this task

Use the following procedure to create a video class of service user template.

### Procedure

1. Log on to System Manager as admin.
2. On the System Manager console, click **Elements** > **Conferencing**.
3. In the Name column on the Conferencing Dashboard, click the Provisioning Client.
4. In the Provisioning Client window, select **System Management** > **Video Class of Service**.
5. Complete the following fields:
    - **Name**: Type the name of Video Class being created.
    - **Maximum average bandwidth per participant (kbps)**: Type a value.
    - **Codec Class**: Select from the list. The parameters for each codec class are shown in the table on the window.

**Note:**

The parameters are automatically calculated when you modify the value in the field for Maximum average bandwidth per participant (kbps).

- **Base resolution**: Select a base resolution from the list.

6. Click **Save**.

### Next steps

Proceed to configuring display numbers in Provisioning Client.

## Configuring display numbers in Provisioning Client

You can configure display numbers from Provisioning Client to manage the access numbers that are displayed in Collaboration Agent.

### About this task

Use the following procedure to configure display numbers in Provisioning Client.

### Procedure

1. Log in to System Manager.
2. On the System Manager console, click **Elements** > **Conferencing**.
3. In the Name column on the Conferencing Dashboard, click the Provisioning Client.

   A new browser window appears and displays the Avaya Aura® Provisioning Client.
4. In the Provisioning Client window, select **System Management > Routing > Service URI**.
5. Click the **Display Numbers** tab.
6. In the **Display Number** field, type a number.
7. In the **Description** field, type a description (maximum 50 characters).
8. Click **Save**.

### Result

The number and description appears in Collaboration Agent instead of the Service URI.

**Related links**

Adding conference access numbers in Provisioning Client on page 313
Deploying the Avaya Aura Conference Manager Add-in for Microsoft Outlook on page 622

# Deleting display numbers in Provisioning Client

### About this task

Use the following procedure to delete display numbers from Provisioning Client.

### Procedure

1. Log in to System Manager.
2. On the System Manager console, click **Elements** > **Conferencing**.
3. In the Name column on the Conferencing Dashboard, click on the Provisioning Client you want to access.

   A new browser window appears and displays the Provisioning Client page.
4. In the Provisioning Client window, select **System Management > Routing > Service URI**.
5. Click the **Display Numbers** tab.
6. Navigate to the display number you want to remove and under the Delete column, click **Delete**.

   The message **Display number deleted successfully** appears.
7. Click **Logout** to exit Provisioning Client.

# Adding a location

### About this task

For any Location you have configured on System Manager (or your PBX equivalent), you must add it manually to Provisioning Client. Use the following procedure to add a location that is being serviced.

### Procedure

1. In the Provisioning Client window, select **System Management > Routing > Locations**.
2. Click **Add Location**.
3. In the Location Name box, enter the name of the location.

   **Important:**

   The name is case-sensitive name and in a Turnkey deployment, this field performs no external validation. Avaya recommends entering the location of the Avaya Aura® Conferencing system. So, for example, if the Avaya Aura® Conferencing system is located in New York, enter `New York`.
4. In the Location Description box, enter any pertinent information about the location.
5. Click **Save**.

6. Repeat Steps 2 through 5 for each location in System Manager.(or your PBX equivalent).

### Next steps

Assign media server clusters to locations or refer back to your checklist for more information about your next task.

## Assigning media server clusters to locations

### About this task

Use the following procedure to assign a media server cluster to serve conference calls for a particular location.

### Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Server Serving Locations** tab.
3. From the Media Server Cluster box, select the media server cluster you want to associate with a location.
4. In the Add locations area, select the check box of the location(s) to which you want to associate the selected media server cluster.
5. Click **Save**.
6. Repeat Steps 3 through 5 to assign other media server clusters.

### Next steps

Assign media server clusters to a physical location.

**Related links**

Assigning a media server cluster to the SBC location on page 459
Assigning media server clusters to a physical location on page 319

## Assigning media server clusters to a physical location

### About this task

A media server cluster must be assigned a physical location for communication with other network elements. Use the following procedure to assign a particular media server cluster to a location.

### Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.

2. Click the **Media Server Cluster Physical Location** tab.
3. From the Select by box, select **Location**.
4. From the Select Physical Location box, select the location to which you want to assign a media server cluster.
5. From the Available Media Server Clusters box, select the appropriate media server cluster, and then click **Copy**. If you want to assign all available media server clusters, click **Copy all**.
6. Click **Save**.
7. Repeat Steps 3 through 6 for each location.

### Next steps

Add the System Manager domain in Provisioning Client or, if this is a Turnkey deployment, refer back to your checklist for more information about your next task.

**Related links**

Assigning a media server cluster to the SBC location on page 459

Assigning media server clusters to locations on page 319

## Making Avaya Aura® Conferencing aware of System Manager domains

In order for Avaya Aura® Conferencing to operate successfully within the Avaya Aura® solution stack, System Manager must make Avaya Aura® Conferencing aware of all SIP domains. In other words, there must be a synchronization between System Manager and Avaya Aura® Conferencing.

When you assign a conference profile to a user, by way of System Manager, and this user has a communication address which does not exist in Avaya Aura® Conferencing, System Manager pushes the user to Avaya Aura® Conferencing and creates the SIP domain on Avaya Aura® Conferencing. However, you may want to add a SIP domain to System Manager and not assign any users to it. In this case, you will require another mechanism for pushing the SIP domain to Avaya Aura® Conferencing.

In all new releases of System Manager, you can configure automatic synchronization. This means that System Manager pushes all new SIP domains to Avaya Aura® Conferencing automatically. Currently, this feature only pushes new SIP domains to Avaya Aura® Conferencing. It does not delete SIP domains. So, if you remove a SIP domain from System Manager, you must also manually remove it from Avaya Aura® Conferencing. If you do not have a new release of System Manager, you must manually add new SIP domains to Avaya Aura® Conferencing, using the Provisioning Client interface.

**Note:**

Automatic synchronization is supported from System Manager 6.3.7 Service Pack 7 + Patch and System Manager 6.3.9 Service Pack 9. If you have an older version, you must manually add new SIP domains using the Provisioning Client interface.

**Related links**

Enabling the automatic synchronization of domains on page 321
Adding System Manager domains in Provisioning Client on page 321
Configuring the route to Avaya Aura Conferencing on System Manager on page 309

## Enabling the automatic synchronization of domains

### About this task

Use this task to configure automatic synchronization of SIP domains between System Manager and Avaya Aura® Conferencing.

### Procedure

1. Ensure that the Avaya Aura® Conferencing Provisioning Client network element has been added to the System Manager inventory.

   For more information, see Configuring the application server network elements on System Manager on page 305.

2. Log on to System Manager and navigate to **Elements** > **Conferencing**.
3. Click **Sync** in the left hand menu.
4. Click **Synchronize Domains** to synchronize new domains.

   System Manager displays a list of pushed domains. If the synchronization is not successful, System Manager displays an error message.

**Related links**

Making Avaya Aura Conferencing aware of System Manager domains on page 320

## Adding System Manager domains in Provisioning Client

### About this task

You must manually add all the System Manager domains into Provisioning Client.

### Procedure

1. In the Provisioning Client window, select **System Management > User Domains**.
2. In the System Manager Domain box, enter the name of the domain you want to add.
3. Click **Add**.

4. Repeat Steps 2 and 3 for each System Manager domain.

### Result

Adding System Manager domains in Provisioning Client is complete.

**Related links**

Making Avaya Aura Conferencing aware of System Manager domains on page 320

## Assigning the conferencing profile to new System Manager users

This procedure only applies to Avaya Aura® deployments. This procedure does not apply to Turnkey deployments.

To use Avaya Aura® Conferencing, a System Manager user must be assigned the conferencing profile. After you assign the conferencing profile to the System Manager user, the user is added into the Avaya Aura® Conferencing database and is available for editing in Provisioning Client.

Avaya Aura® Conferencing SIP users using SIP services require a Session Manager profile to be assigned.

The conferencing profile specifies conferencing parameters, such as participant and moderator collaboration codes and pass codes, location, and conferencing user data template for a user.

### Before you begin

Ascertain if the new user you are adding is using a SIP endpoint or a non-SIP endpoint as this determines how to configure the Communication Profile.

### About this task

Use the following procedure to assign the conferencing profile to a new System Manager user.

**Note:**

If you are using the LDAP directory integration feature, do not perform this feature. See *Deploying Avaya Aura® Conferencing* at the Avaya Support website: http://support.avaya.com.

### Procedure

1. On the System Manager console, click **Users** > **User Management**.
2. In the navigation pane, click **User Management** > **Manage Users**.
3. On the User Management page, click **New**.

   The New User Profile page appears.
4. On the **Identity** tab, complete the required information, and then click **Commit & Continue**.

5. On the **Communication Profile** tab, complete the required information.
    a. **Name**: Type a name.
    b. **Default**: Select this check box.
    c. Complete the **Communication Address** section to add your E.164 or private enterprise numbering plan.
    d. Complete the **Session Manager Profile** section.
    e. Complete the following profiles as required for your users:
        - **CM Endpoint Profile**
        - **CS 1000 Endpoint Profile**
        - **Messaging Profile**
        - **CallPilot Messaging Profile**
        - **IP Office Endpoint Profile**
        - **Presence Profile**
    f. Complete the **Conferencing Profile** section, proceed to Step 6 on page 323.
6. On the **Communication Profile** tab, select the **Conferencing Profile** check box.

    The Conferencing Profile section expands.
7. Complete the following fields:
    - **Select Auto-generated Code Length**: Modify the PIN length from 6 to 8 characters, default is 6.
    - **Auto Generate Participant Collaboration Code**: Select this check box if you want the system to automatically generate the collaboration codes for the participant.
    - **Participant Collaboration Code**: If you want to assign a specific participant collaboration code for this user, make sure the **Auto Generate Participant Collaboration Code** check box is not selected, and type the conference participant collaboration code for this user in the **Participant Collaboration Code** box.
    - **Auto Generate Moderator Collaboration Code**: Select this check box if you want the system to automatically generate the collaboration codes for the moderator.
    - **Auto Generate Participant Pass Code**: Select this check box if you want the system to automatically generate the pass codes for the participant.

        **Note:**

        Pass codes are like a second level of security. Participants must enter pass codes after they enter the collaboration code, in order to access the conference. Moderators must send the code to the participants.
    - **Auto Generate Moderator Pass Code**: Select this check box if you want the system to automatically generate the pass codes for the moderator.

- **Location**: Select a location from the list. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users.

  **Note:**

  For SIP users, the location value is obtained from the Home Location field in the Session Manager profile (if an appropriate value was not selected in the Location field in the Conferencing Profile).

- **Template**: Select the Avaya Aura® Conferencing template you want to assign to this user. The settings for the selected template display. If you are running System Manager 6.3.3 or earlier, you can click the Get Templates button. This button is no longer displayed on System Manager 6.3.4 and later.

8. Click **Commit & Continue**.
9. Repeat Steps 1 on page 322 through 8 on page 324 for each new user you want to add to System Manager and assign the conferencing profile.

### Result

Avaya Aura® Conferencing is assigned to a new System Manager user.

## Assigning the conferencing profile to existing System Manager users

This procedure only applies to Avaya Aura® deployments. This procedure does not apply to Turnkey deployments.

To use Avaya Aura® Conferencing, a System Manager user must be assigned the conferencing profile. The conferencing profile specifies conferencing parameters, such as participant and moderator collaboration codes and pass codes, location, and conferencing user data template for a user. After you assign the conferencing profile to the System Manager user, the user is added into the Avaya Aura® Conferencing database and is available for editing in Provisioning Client.

Avaya Aura® Conferencing SIP users using SIP services require a Session Manager profile to be assigned.

### Before you begin

- Ascertain if the user you are modifying is using a SIP endpoint or a non-SIP endpoint as this determines how to configure the Communication Profile.
- Ensure a Communication Profile has already been configured in System Manager for the existing user.

### About this task

Use the following procedure to assign the conferencing profile to an existing System Manager user.

**Note:**

If you are using the LDAP directory integration feature, do not perform this feature. See *Managing LDAP directory integration*.

### Procedure

1. On the System Manager console, click **Users** > **User Management**.
2. In the navigation pane, click **Manage Users**.
3. Select the check box for the user you want to assign the conferencing profile, and click **Edit**.
4. On the **Communication Profile** tab, select the **Conferencing Profile** check box.

   The Conferencing Profile section expands.
5. Complete the following fields:
   - **Select Auto-generated Code Length**: Modify the PIN length from 6 to 8 characters, default is 6.
   - **Auto Generate Participant Collaboration Code**: Select this check box if you want the system to automatically generate the collaboration codes for the participant.
   - **Participant Collaboration Code**: If you want to assign a specific participant collaboration code for this user, make sure the **Auto Generate Participant Collaboration Code** check box is not selected, and type the conference participant collaboration code for this user in the **Participant Collaboration Code** box.
   - **Auto Generate Moderator Collaboration Code**: Select this check box if you want the system to automatically generate the collaboration codes for the moderator.
   - **Auto Generate Participant Pass Code**: Select this check box if you want the system to automatically generate the pass codes for the participant.

     **Note:**

     Pass codes are like a second level of security. Participants must enter pass codes after they enter the collaboration code, in order to access the conference. Moderators must send the code to the participants.
   - **Auto Generate Moderator Pass Code**: Select this check box if you want the system to automatically generate the pass codes for the moderator.
   - **Location**: Select a location from the list. This field is mandatory for non-SIP users without a Session Manager profile and optional for SIP users.

     **Note:**

     For SIP users, the location value is obtained from the Home Location field in the Session Manager profile (if an appropriate value was not selected in the Location field in the Conferencing Profile).
   - **Template**: Select the Avaya Aura® Conferencing template you want to assign to this user. The settings for the selected template display. If you are running System Manager

6.3.3 or earlier, you can click the Get Templates button. This button is no longer displayed on System Manager 6.3.4 and later.

6. Click **Commit & Continue**.
7. Repeat Steps 1 on page 325 through 6 on page 326 to assign the conferencing profile for every existing System Manager user.

# Assigning the conferencing profile to a group of System Manager users

This procedure only applies to Avaya Aura® deployments. This procedure does not apply to Turnkey deployments.

To use Avaya Aura® Conferencing, a System Manager user must be assigned the conferencing profile. The conferencing profile specifies conferencing parameter such as moderator and participant collaboration codes and pass codes, location, and conferencing user data template for a user.

Avaya Aura® Conferencing SIP users using SIP services require a Session Manager profile to be assigned.

## About this task

Use the following procedure to assign the conferencing profile to a group of System Manager users.

**Note:**

Avaya recommends using this procedure when assigning conferencing profiles to a large group of System Manager users.

**Note:**

If you are using the LDAP directory integration feature, do not perform this feature. See *Deploying Avaya Aura® Conferencing* at the Avaya Support website: http://support.avaya.com.

## Procedure

1. On the System Manager console, click **Users** > **User Management**.
2. In the navigation pane, click **Manage Users** and ensure there is at least one user on this page.
3. In the **Communication Address** section, verify that at least one communication address is assigned.
4. In the **Session Manager Profile** section, verify that at least one Session Manager profile is assigned.
5. Log on to the System Manager as admin through ssh.

6. Run the following commands:
   - For System Manager 6.3:

     ```
     cd $MGMT_HOME/bulkadministration/exportutility
     ```

     and

     ```
     bash exportUpmUsers.sh
     ```
   - For System Manager 6.2:

     ```
     cd $MGMT_HOME/upm/bulkexport/exportutility
     ```

     and

     ```
     bash exportUpmUsers.sh
     ```

   Job:<filename> is created.
7. Copy the <filename>.zip, as shown in the previous step to your PC.
   - For System Manager 6.3, <filename>.zip is located in `$MGMT_HOME/bulkadministration/export`.
   - For System Manager 6.2, <filename>.zip is located in `$MGMT_HOME/upm/bulkexport`.
8. View `$AVAYA_LOG/mgmt/um_bulkexport/bulkexportTraceLog.log` file to check for error messages.
9. Extract the xml file(s) from <filename>.zip on your PC.
10. In the xml file(s), remove all users who are not affected.
11. In the xml file(s), locate the following information:

    ```
    <tns:users xmlns:tns="http://xml.avaya.com/schema/import"
    xmlns:ns3="http://xml.avaya.com/schema/import1"
    xmlns:ns4="http://xml.avaya.com/schema/deltaImport"
    xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://xml.avaya.com/schema/import userimport.xsd">
    ```
12. In the xml file(s), replace the information specified in Step 11 with the following information:

    ```
    <tns:deltaUserList xmlns:ns3="http://xml.avaya.com/schema/import1"
    xmlns:tns="http://xml.avaya.com/schema/deltaImport"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://xml.avaya.com/schema/deltaImport userdeltaimport.xsd ">
    ```
13. In the xml file(s), perform the following steps:
    a. Replace all instances of `<tns:user>` with `<tns:userDelta>`.

    b. Replace all instances of `</tns:user>` with `</tns:userDelta>`.

    c. Replace all instances of `<tns:users>` with `<tns:deltaUserList>`.

    d. Replace all instances of `</tns:users>` with `</tns:deltaUserList>`.

14. In the xml file(s), add the following xml segments between the lines `<commProfileList>` and `</commProfileList>` for users who have a conferencing profile:

    ```
    <commProfile xsi:type="ns2:MmcsCommProfileType" xmlns:ns2="http://xml.avaya.com/
    schema/import_mmcs">
    <commProfileType>mmcsCommProfile</commProfileType>
    <ns2:template>template</ns2:template>
    <ns2:securityCode>123456</ns2:securityCode>
    <ns2:moderatorPin>654321</ns2:moderatorPin>
    <ns2:eventConfCode>222</ns2:eventConfCode>
    <ns2:location>location</ns2:location>
    <ns2:autoGeneratedCodeLength>6</ns2:autoGeneratedCodeLength>
    </commProfile>
    ```

15. To create a conferencing profile from an existing template, copy the template and add the xml segments from the preceding step to the conferencing profile xml file.
16. Verify that all SIP users have values for `primarySM` and `homeLocation`.
17. Verify that all users have at least one handle in `commProfileSet > handleList`.
18. Complete the conferencing profile xml values:

    Where:

    - *template*: is an Avaya Aura® Conferencing user template name.
    - *securityCode*: is a Participant collaboration code. This is required if the autoGeneratedCodeLength parameter is not configured.
    - *moderatorPin*: is a Moderator collaboration code. This is required if the autoGeneratedCodeLength parameter is not configured.
    - *eventConfCode*: is a Presenter security code. This is required if the autoGeneratedCodeLength parameter is not configured.
    - *autoGeneratedCodeLength*: indicates if security codes must be auto generated and the required length for auto generated codes.
    - *location*: is an Avaya Aura® Conferencing user Location. The location is mandatory for non-SIP users without a configured Session Manager profile and optional for SIP users.

      **Note:**

      For SIP users, the value for the Avaya Aura® Conferencing user location is obtained from the Home Location parameter in the Session Manager profile (if the Location parameter in the Conferencing Profile is not configured).

19. Log on to System Manager as admin.
20. On the System Manager console, click **Bulk Import and Export**.
21. On the Import and export page, click **Import**.
22. On the Import page, click **User Management**.
23. On the Import - User and global settings page, click **Users**.
24. On the Import users page, click **Browse** to select the edited xml file.

25. In the General section on the Import users page, set Select import type to **Partial**.
26. Click **Import** to start the job.
27. In the **Manage job** section, click **Refresh** to view the status of your job.

    The status updates to indicate SUCCESSFUL or FAILED.

    ✱ **Note:**

    In case of a failure, under the **Job name** column, click the job number to see the error message.

# Verifying access to the MeetMe conference

## Before you begin

You must have Avaya Equinox for Windows installed and configured on a PC. To install and configure Avaya Equinox for Windows, see *Implementing Avaya Equinox for Windows*.

## About this task

Use this procedure to verify that you can access the MeetMe conference URI.

## Procedure

1. Start Avaya Equinox for Windows.
2. Click **Settings**.
3. In navigation pane in the **General Settings** dialog box, click **Server**.
4. On Server page, complete the following fields:
    - **Server address**: Input your server.
    - **Server port**: 5061 for TLS or 5060 for TCP.
    - **Transport type**: Check TLS or TCP.
5. In navigation pane in the General Settings dialog box, click **Dialing Rules**.
6. On the Dialing Rules page, clear the **Apply Dialing Rules for outgoing calls** check box to prevent dialing rules from being applied to the number dialed to access the MeetMe conference.
7. In the navigation pane, click **Conference**.
8. In the Conference Factory URI box on the Conference page, type the Adhoc URI you entered in Provisioning Client.
9. Click **OK**.
10. In the Extension box, enter a valid communication profile name that is administered on System Manager.

11. In the Password box, enter the password for the communications profile.
12. Click **Log in**.
13. Click **Call**.
14. On the dialpad, enter the MeetMe number you configured in Provisioning Client.
15. On the dialpad, click **Call**.

    You hear the Avaya introduction and are prompted to enter your conference access code followed by the pound (#) key.
16. Click **Keypad**.
17. On the keypad, enter a valid moderator PIN and press the pound (#) key.

    The MeetMe conference starts.

# Associating Web conferencing resources with a location in Provisioning Client

### Before you begin

Web conferencing server resources (that is, Web Conferencing Server and Document Conversion Server) must be configured on the Element Manager Console.

### About this task

Perform this procedure to associate Web conferencing resources with a location. You can associate multiple locations with the Web Conferencing Server resources.

### Procedure

1. In the Provisioning Client window, select **System Management > Routing > Web Conferencing Server Resources**.
2. From the Location box, select the location to which you want to associate Web Conferencing Server resources.
3. From the Available WCS Clusters box, select the appropriate WCS server cluster, and then click **Copy**. If you want to assign all available WCS server clusters, click **Copy all**.
4. From the Document Conversion Server box, select the Document Conversion Server for the selected location.
5. Click **Save**.
6. Repeat this procedure for every location you previously defined.

# Configuring a Web conferencing host

This task is particularly significant if you plan to deploy the Avaya Aura® Conference Manager Add-in for Microsoft Outlook®. You will require the Web conferencing host name during the configuration of the Avaya Aura® Conference Manager Add-in for Microsoft Outlook®.

### About this task

Use the following procedure to configure a Web conferencing host name.

### Procedure

1. In the Provisioning Client window, select **System Management** > **Routing** > **Collaboration Agent Service FQDN**.
2. In the FQDN field, enter an FQDN name.

   Depending on the deployment type, you should enter either:

   - The fully qualified domain name (FQDN) of the Provisioning Manager network element/ Collaboration Agent network element.
   - The FQDN of the load balancer.
3. Click **Save**.

**Related links**

Deploying the Avaya Aura Conference Manager Add-in for Microsoft Outlook on page 622
Implementing a ClickOnce deployment on page 623
Implementing a centralized software deployment on page 625

# Configuring an operator

An operator has the following abilities:

- search conferences in Collaboration Agent by user name and participant code
- log on to a conference using the moderator code
- has moderator privileges during a conference

### About this task

Use the following procedure to configure a user as an operator of a conference.

### Procedure

1. In the Provisioning Client window, select **User Management** > **Conferencing User.**
2. In the **Select Login name** field, type a logon name, and click **>>**.
3. Select the **Enable operator control** check box to enable, and click **Save**.

# Configuring the system operator

### Before you begin

You can only specify one URI for the operator.

### About this task

Use this procedure to specify the URI that is contacted when a participant requests the operator during a conference.

### Procedure

1. In the Provisioning Client window, select **System Management** > **System Default Settings**.
2. In the **Operator** field, enter the URI of the operator. If a participant requests the operator during a conference, this URI is contacted.
3. Click **Save**.

# Configuring media server clusters for event conferences

Event conferences are very large conferences that are used for gathering 100s or possibly 1000s of participants, often from multiple global locations. Event conferences are used for company announcements, town hall meetings, and so on. For more information about event conferences, see Event conferencing and media cascading on page 45 and Event conferencing considerations on page 54.

### About this task

Use the following procedure to configure a large event conference.

### Procedure

1. In the Provisioning Client window, select **User Management** > **User Template**.
2. In the User Template window, complete the following fields:
    - **Name**: Type a name.
    - **Conference class of service**: Select an event name from the list, for example, Event_1000 or Event_2000.
    - **Enable Video**: Select the check box to enable.
    - **Priority**: Select a priority type from the list.
3. Click **Save**.
4. In the Provisioning Client window, select **System Management** > **Routing** > **Media Server Resources**.
5. Click the **Media Server Serving Locations** tab.

6. In the Add locations section, clear the check boxes for the locations where event conferencing is to be used.
7. Click **Save**.
8. Click the **Media Server Cluster Physical Location** tab.
9. In the **Select by** field, select **Location** from the list.
10. In the **Select Physical Location** field, select the location for where the equipment is located.
11. In the **Available Media Server Clusters** list, select the **Media Server Cluster**, and click **Copy** to move it to the **Select Media Server Clusters** list. If you want to assign all available media server clusters, click **Copy all**.
12. Click the **Media Server Clusters for Event Conferences** tab.
13. In the **Available Media Server Clusters** list, select the **Media Server Cluster**, and click **Copy** to move it to the **Select Media Server Clusters** list.
14. Click **Save**.
15. If the Event conferencing Service URI is not already added, see Adding MeetMe Adhoc and Event service URIs in Provisioning Client on page 313.

### Next steps

Proceed to configuring media server cascading.

**Related links**

Configuring WCS clusters for event conferences on page 256
Event conferencing and media cascading on page 45

## Configuring Avaya Aura® Media Server cascading

Traffic can be minimized between Avaya Aura® Media Servers if a conference has users on different Avaya Aura® Media Servers. Only one channel is used between Avaya Aura® Media Servers.

For more information on the available hardware options for cascading servers, check the latest list of supported hardware.

### Before you begin

You must configure more than one Media Server cluster in Element Manager.

### About this task

Use the following procedure to configure Avaya Aura® Media Server cascading.

### Procedure

1. In the Provisioning Client window, select **System Management** > **System Default Settings**.
2. On the **System Default Settings** tab, select the **Allow media cascading** check box to enable.
3. Click **Save**.
4. In the Provisioning Client window, select **System Management** > **Routing** > **Media Server Resources**.
5. Click the **Media Server Serving Locations** tab.
6. In the Media Server cluster box, select a Media Server cluster from the list.
7. In the Add locations section, select a location check box to assign a location for the Media Server cluster.
8. Click **Save**.
9. Repeat Steps 6 through 8 for each Media Server cluster.
10. Click the **Media Server Cluster Physical Location** tab.
11. In the Select by field, select **Location** from the list.
12. In the Select Physical Location field, select a location from the list.
13. Click **Save**.
14. Click the **Media Stream Cascading** tab.
15. In the Select location field, select a location from the list.
16. Select the check box to enable **Cascading is allowed when this location is hosting the conference**.
17. Click **Save**.
18. Repeat Steps 15 through 17 for each location.
19. Click the **Hosting Locations** tab.
20. In the Select Hosting Location field, select a hosting location as the host for all other locations.
21. Click **Copy all** to move the locations in the Hostable Locations field to the Hosted Locations field.
22. Click **Save**.

### Next steps

Proceed to configuring bandwidth management.

#### Related links

Configuring the codecs for the cascading trunks on page 335

## Configuring the codecs for the cascading trunks

### About this task

Use this task to specify a G.711, G.722, or G.726 audio codec for the cascading trunks in your deployment. If you are using cascading trunks in your deployment, you can also specify the packet time for the audio codec. If you are not using cascading trunks in your deployment, the packet time is hardcoded to 20 milliseconds.

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Cascading Trunk Codec Settings**.
2. On the **Cascading Trunk Codec Settings** dialog, re-order the list of audio codecs in accordance with your preferences.
3. Specify the packet time for the audio codec from the **Default PTimes for all codecs** drop-down list.
4. Click **Ok**.

**Related links**

Configuring Avaya Aura Media Server cascading on page 333
Cascading Trunk Codec Settings field descriptions on page 335

## Cascading Trunk Codec Settings field descriptions

| Name | Description |
|---|---|
| **Enabled** | The Enabled panel lists the audio codecs that are available. You can select each item in this list. |
| **Default PTimes for all codecs** | Specify a packet time for the audio codec. By default, the packet time is set to 10 milliseconds. |

| Button | Description |
|---|---|
| **Up** | Moves the selected audio codec to a higher location on the list. |
| **Down** | Moves the selected audio codec to a lower location on the list. |
| **Ok** | Click **Ok** to apply your changes. |
| **Cancel** | Click **Cancel** to disregard your changes. |

**Related links**

Configuring the codecs for the cascading trunks on page 335

# Configuring a regional cascading location

## Before you begin

- You must be logged into Provisioning Client.
- Cascaded locations (that is, locations that cascade through a cascading location) must have a good-quality WAN link.
- Cascaded locations do not need to have media servers configured.
- A cascaded location can be assigned to only one cascading location (that is, the location that provides media cascading).
- A cascaded location and cascading location pair cannot be assigned as a hosted location and hosting location pair (and vice versa).
- A cascading location can be the same as the hosting location for a particular location.
- Cascading must be enabled for the Avaya Aura® Conferencing system, the user location, the cascading location, and the hosting location if you want to use regional cascading.
- For Event conferences, the hosting media servers are dedicated Event conference servers. The cascading media servers are not dedicated. In other words, any media servers that are assigned to serve a certain location can be used for media cascading.

## About this task

Use this procedure to configure a regional cascading location, which provides media cascading to the remote locations you specify. The users at the specified locations will be able to call into the regional cascading location instead of the joining the conference directly via the hosting media server. Regional cascading locations enable you to optimize WAN bandwidth usage.

**Note:**

Cascading must be allowed (enabled) for the Avaya Aura® Conferencing system, the user location, the cascading location, and the hosting location if you want to use regional cascading.

## Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Cascading Locations** tab.
3. From the Select Cascading Location box, select the location that will provide media cascading for other locations.
4. From the Locations that have no Cascading Location assigned list box, select the location(s) that you want to assign to the selected cascading location, and then click **Copy**. If you want to assign all locations, click **Copy all**. For more information see, Media Cascading Locations tab field descriptions on page 337.
5. Click **Save**.

**Related links**

Media Cascading Locations tab field descriptions on page 337

## Media Cascading Locations tab field descriptions

| Name | Description |
|---|---|
| **Select Cascading Location** | Select the location that will provide media cascading for other locations. |
| **Locations that have no Cascading Location assigned** | Displays the locations that you can assign to the selected cascading location. From this list box, you can select the location(s) that you want to assign to the selected cascading location. |
| **Locations that cascade through *<selected cascading location>*** | Displays the locations that you want to assign to the selected cascading location. The selected cascading location is a variable/dynamic field, based on the **Select Cascading Location** field. |

| Button | Description |
|---|---|
| **Copy all** | Moves all of the locations displayed in the Locations that have no Cascading Location assigned list box into the Locations that cascade through list box. |
| **Copy** | Moves the selected location in the Locations that have no Cascading Location assigned list box into the Locations that cascade through list box. |
| **Remove** | Moves the selected location in the Locations that have no Cascading Location assigned list box into the Locations that cascade through list box. |
| **Remove All** | Moves all of the locations displayed in the Locations that cascade through list box into the Locations that have no Cascading Location assigned list box. |

**Related links**

Configuring a regional cascading location on page 336

# Configuring bandwidth management

Bandwidth for conferences can be managed in accordance with configured thresholds and user priority. With proactive bandwidth optimization, you can reduce bandwidth usage and reduce costs while managing the quality of multimedia sessions.

### About this task

Use the following procedure to configure bandwidth management.

## Procedure

1. In the Provisioning Client window, select **System Management** > **System Default Settings**.
2. Select the **Allow bandwidth management** check box to enable.
3. Click **Save**.
4. In the Provisioning Client window, select **System Management** > **Bandwidth Optimization**.
5. In the Select location field, select a location from the list.
6. In the High threshold field, type a value. The range is 75 to 100. If 100 is selected, bandwidth optimization is disabled for all new and existing sessions.
7. In the Critical threshold field, type a value. The range is 75 to 100. If 100 is selected, bandwidth optimization is disabled for all new sessions. The value must be greater than the High threshold value.
8. Click **Save**.
9. Select **User Management** > **Conferencing User**.
10. In the **Select login name** field, type a login name, for example, jsmith@yourcompany.com, and click **>>**.
11. In the **Priority** field, select one of the following:
    - Business critical
    - High
    - Medium
    - Low
12. In the **Class of service** field, assign the conference class of service for this user.

    For more information about the default classes of service, see Creating a conference class of service user template on page 315.
13. Select the **Enable Video** check box to enable video for this user.
14. Click **Save**.

# Chapter 21: Configuring the recording feature

Avaya Aura® Conferencing captures audio and web collaboration within a conference. Avaya Aura® Conferencing does not record video and it does not record standalone web conferences (SWC). Standalone web conferences are conferences that do not have an Avaya Aura® Conferencing audio component. Instead, their audio component is provided by an external source, such as a direct call between two parties.

Avaya Aura® Conferencing supports the following recording deployments:

- SMB or medium deployment. See Checklist for configuring recording in an SMB or medium deployment on page 341.
- Dedicated Recording server deployment. See Checklist for configuring recording in a dedicated recording server deployment on page 341.

Avaya Aura® Conferencing does not implement a quota system. So, for example, the recordings of a single user could take up all of the available storage space.

Avaya Aura® Conferencing provides encryption for stored recordings on the hard drive. To enable encryption, you must choose encryption as an option at installation time. For more information, see, Encrypting the recording data disk  on page 131. If you do not choose encryption as an option at installation time, recordings are stored and played back without encryption. In all cases, recordings are encrypted in transit, including for playback, assuming TLS encryption has been enabled for the system.

Users cannot edit recordings except to change the title, and they cannot search for a phrase within a recording.

**Related links**

Conference recording on page 340
Checklist for configuring recording in a dedicated recording server deployment on page 341
Checklist for configuring recording in an SMB or medium deployment on page 341
Dedicated recording server deployment only on page 342
SMB or medium deployments only on page 346
Both deployments on page 347

# Conference recording

## Capacity

### How many hours of storage do the recording server(s) provide?

In terms of recording hours, capacity is a function of what is being recorded. The best case is audio-only and the worst case is audio with screen sharing with lots of movement. The table below defines the recording capacity per recording server. You can deploy multiple recording servers. The key here is that one recording server is permitted per location (physical or virtual). Users are assigned to a particular recording server based on their location as defined within Avaya Aura® System Manager or a Turnkey equivalent. Older releases of Avaya Aura® Conferencing supported the 900Gbyte server. Newer releases of Avaya Aura® Conferencing introduce optional support for a 1.8Tbyte server.

**Table 23: Capacity**

| Type of Media | Format | Size (MB/Hour) | Capacity on the 1.8Tbyte system (Hours) | Capacity on the 900Gbyte system (Hours) |
|---|---|---|---|---|
| **Audio Only Recording** | mp3 | 40 | 45000 | 22000 |
| **Audio + Web (50% slides 50% screen share)** | swf | 72 | 25000 | 12000 |
| **Audio + Web (100% screen share, with movement)** | swf | 105 | 17000 | 8000 |

## Archives

### How are archived recordings, that are stored to external storage, accessed and retrieved? Through the application, directly from the external storage?

In terms of archiving and playback:

- Users can view recordings using the Avaya Aura® Conferencing playback infrastructure, by reaching the recording by way of the URL
- Administrators can configure the backup schedule to automatically backup the recordings daily to the external system.
- Administrators can restore the recordings by choosing from several options: Restore a single recording, all recordings for a given user, or all recordings in the backup folder
- Users can download the recording as audio (.mp3) or audio+web (.swf) and store it anywhere.
- You cannot view recordings that are not in the recording media server, even if they are archived. To view them again, you must restore them.

**Note:**

These downloads don’t have the robust playback capabilities of the native Avaya Aura® Conferencing playback experience e.g. time line, activity stream, and so on.

**Related links**

Configuring the recording feature on page 339

# Checklist for configuring recording in a dedicated recording server deployment

The following checklist provides a high-level view of the tasks involved in configuring the Recording feature in a dedicated Recording server deployment.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Add and configure a media server dedicated for Recording via Element Manager Console. | See Adding a media server dedicated for recording on page 342. | | |
| 2 | Assign locations to the Recording media server cluster via Provisioning Client. | See Configuring the Recording media server cluster for locations on page 348. | | |
| 3 | Create and assign a certificate for the dedicated Recording server. | See Creating a certificate for a dedicated Recording server on page 345. | | |
| 4 | Configure the system-wide Recording setting via Provisioning Client. | See Configuring the system-wide Recording setting on page 349. | | |
| 5 | Configure the Recording feature for users via Provisioning Client. | See Configuring the Recording feature for a user on page 349. | | |
| 6 | Configure the Recording backup server. | See Configuring the Recording backup server on page 353. | | |

**Related links**

Configuring the recording feature on page 339

# Checklist for configuring recording in an SMB or medium deployment

The following checklist provides a high-level view of the tasks involved in configuring the Recording feature in an SMB or medium deployment.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Configure the Recording media server cluster via Element Manager Console. | See Configuring Recording for a media server cluster in aan SMB or medium deployment on page 347. | | |
| 2 | Configure the system-wide Recording setting via Provisioning Client. | See Configuring the system-wide Recording setting on page 349. | | |
| 3 | Assign a Recording media server cluster to locations. | See Assign a Recording media server cluster to locations  on page 348. | | |
| 4 | Configure the Recording feature for users via Provisioning Client. | See Modifying a single user on page 349. | | |
| 5 | Configure the Recording backup server. | See Configuring the Recording backup server on page 353. | | |

**Related links**

Configuring the recording feature on page 339

# Dedicated recording server deployment only

In this context, a dedicated recording server deployment is also known as a large deployment. For previous releases, it was called a ‘standalone” deployment.

The steps involved in configuring recording for a dedicated recording server deployment are much the same as the steps involved in configuring recording for an SMB or medium deployment. However, the following procedures only apply to dedicated recording server deployments.

**Related links**

Configuring the recording feature on page 339
Adding a media server dedicated for recording on page 342
Creating and importing a certificate for the dedicated recording server on page 345

## Adding a media server dedicated for recording

### About this task

Use this procedure to add a media server that will be dedicated for recording.

**Note:**

During this procedure, you will create a new media server cluster. A media server cluster supports a maximum of eight media servers:

- one primary
- one secondary
- six standard servers

## Procedure

1. In the navigation pane of Element Manager Console, click **Addresses**.
2. In the Addresses window, click **Add (+)**.
3. In the Add IPv4 Address dialog box, enter the logical name and IP address for the media server.
4. Click **Apply**.
5. In the navigation pane of Element Manager Console, click **Servers**.
6. In the Servers window, click **Add (+)**.
7. In the Add Server dialog box, complete the following fields:
    - **Short Name**
    - **Long Server Name**
    - **Internal OAM (Default) Address**: Enter the IP address you specified in Step 3.
    - **Operating System**: Select **linux**.
    - **Host Name**: Enter the short name or FQDN of the server.
8. Click **Apply**.
9. In the navigation pane of Element Manager Console, click **Feature Server Elements > Media Servers and Clusters > Media Servers**.
10. In the Media Servers window, click **Add (+)**.
11. In the Add Media Server dialog box, complete the following fields:
    - **Short Name**
    - **Long Name**
    - **Base Port**: Type 49000.
    - **Enable SIP TCP**: Select this check box to enable.

      **OR**

      **Enable SIP TLS**: Select this check box to enable.
    - **SIP Certificate**: If SIP TLS is enabled, select the certificate you want to use for SIP TLS. For more information, see the chapter for Configuring Transport Layer Security.

**Note:**

Accept the default for all other fields.

12. Click **Apply**.
13. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers** > **<media server you specified in Step 3> Instance**.
14. In the Media Server Instance window, click **Add (+)**.
15. In the Add Media Server Instance dialog box, complete the following fields:
    - **Server**: Select the media server you created in Step 3.
    - **Load or Patch**: Select the software load.
    - **Engineering**: Select the configuration that corresponds to your hardware type and layout.
16. Click **Apply**.
17. In the navigation pane of Element Manager Console, click **Feature Server Elements > Media Servers and Clusters > Media Server Clusters**.
18. In the Media Server Clusters window, click **Add (+)**.
19. In the Add Media Server Cluster dialog box, complete the following fields:
    - **Short Name**
    - **Long Name**
    - **Primary Server**: Select the Avaya Aura® Media Server network element. This list contains only the media server network elements that do not belong to any cluster. You must specify a primary server.
    - **Secondary Server**: If this cluster has two or more Avaya Aura® Media Servers, you must specify a secondary server. Otherwise, leave this field blank.
    - **Role**: Select **RECORDING ONLY**.
20. Click **Apply**.
21. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers** > **MediaServer2** >**NE Maintenance**.
22. In the Media Server Maintenance dialog box, select the row for ID 0.
23. Click **Deploy**.

    The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.
24. Click **Start**.

The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

Check the state transitions for the following fields:

| Field | Status |
|---|---|
| Maint | None |
| Admin | Online |
| Link | Up |
| Oper | Active |

25. In the navigation pane of Element Manager Console, click **Feature Server Elements > Media Servers and Clusters > Media Server Clusters**.
26. In the Media Server Clusters window, select **MediaServer1**, and click **Edit (+/-)**.
27. In the Edit Media Server Cluster dialog box, make sure the Role box is set to **CONFERENCING ONLY** .

**Related links**

Dedicated recording server deployment only on page 342

## Creating and importing a certificate for the dedicated recording server

### Before you begin

You must know the enrollment password as completed in Obtaining enrollment password from System Manager on page 564.

### About this task

Use this procedure to create a new certificate for the dedicated Recording server. This procedure creates a passport for the server and assumes that the System Manager is acting as the passport office. If you are using another authority as the passport office, see Introduction to certificates on page 552.

### Procedure

1. In the navigation pane of Element Manager Console, click **Security** > **Certificate Management** > **Enrollment Request**.
2. In the Certificate Enrollment window, complete the following fields:
    - **Logical Name**: Type a logical name for the certificate to be assigned to the dedicated Recording server (for example, AMS2Cert).
    - **Bit length**: Select 1024, 2048, or 4096 from the list. If your security policy does not specify bit length, select **1024**.
    - **Common name**: Type the IP address.

- **Enrollment password**: This password must match the current Enrollment Password that is configured on System Manager.

3. Click **Submit**.

   The certificate is automatically installed on the Element Manager Keystore.

4. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers**.
5. In the Media Servers window, select the dedicated Recording server.
6. Click **Edit (-/+)**.
7. In the Edit Media Server dialog box, complete the following fields:
   - **SOAP/TLS checkbox**: Enable this checkbox.
   - **SIP TLS checkbox**: Enable this checkbox.
   - **SIP Certificate**: Select the certificate you created from the list. This list corresponds to the logical names in the Keystore (for example, AMS2Cert).
   - **SOAP Certificate**: Select the certificate you requested from the list. This list corresponds to the logical names in the Keystore (for example, AMS2Cert).
8. Click **Apply**.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

**Related links**

Dedicated recording server deployment only on page 342

## SMB or medium deployments only

The steps involved in configuring recording for an SMB or medium deployment are much the same as the steps involved in configuring recording for a dedicated recording server deployment. However, the following procedure only applies to an SMB or medium deployments.

**Related links**

Configuring the recording feature on page 339

Configuring recording for a media server cluster in an SMB or medium deployment on page 347

## Configuring recording for a media server cluster in an SMB or medium deployment

### About this task

Use this procedure to assign the Conferencing and Recording Role to a media server cluster in an SMB or medium deployment. This task applies to SMB or medium deployments which provide redundancy and SMB or medium deployments that do not provide redundancy. These non-redundant deployments are called simplex deployments. Avaya Aura® Conferencing provides redundancy using additional servers and a load balancer. In a redundant deployment, the main media server and additional secondary/back-up media servers are in a single cluster.

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters**.
2. In the Media Server Clusters window, select the media server cluster, and click **Edit (+/-)**.
3. From the Role box in the Edit Media Server Cluster dialog box, select **CONFERENCING AND RECORDING**.
4. Click **Apply**.

**Related links**

SMB or medium deployments only on page 346

# Both deployments

The following procedures apply to dedicated recording server and SMB or medium deployments.

**Related links**

Configuring the recording feature on page 339
Assign a Recording media server cluster to locations on page 348
Configuring the Recording media server cluster for locations on page 348
Configuring the system-wide Recording setting on page 349
Configuring the recording feature for users on page 349
Configuring the Recording backup server on page 353
Configuring codecs for recording on page 356
Web Conferencing Server (WCS) clusters on page 249

## Assign a Recording media server cluster to locations

### About this task

Use this procedure to assign a Recording media server cluster to locations.

### Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Server Cluster for Recording** tab.
3. From the Select by box, select **Media Server Cluster**.
4. From the Select Recording Media Server Cluster box, select the appropriate Recording media server cluster.
5. In the Select Locations area, select the check box for each location you want to assign to the selected Recording media server cluster.
6. Click **Save**.

### Related links

Both deployments on page 347

## Configuring the Recording media server cluster for locations

### About this task

Use this procedure to configure and assign a Recording media server cluster to locations.

### Procedure

1. In the Provisioning Client window, select **System Management > Routing > Media Server Resources**.
2. Click the **Media Server Cluster Physical Location** tab.
3. From the Select by box, select **Location**.
4. From the Select Physical Location box, select the location to which you want to assign the Recording media server cluster.
5. From the Available Media Server Clusters box, select the Recording media server cluster (MediaServerCluster2), and then click **Copy**.
6. Click **Save**.
7. Click the **Media Server Cluster for Recording** tab.
8. From the Select by box, select **Media Server Cluster**.
9. From the Select Recording Media Server Cluster box, select the Recording media server cluster you created (MediaServerCluster2).

10. In the Select Locations area, select the check box for each location you want to assign to the selected Recording media server cluster.
11. Click **Save**.

**Related links**

Both deployments on page 347

## Configuring the system-wide Recording setting

### Before you begin

You must be logged into Provisioning Client.

### About this task

Use this procedure to enable the system-wide setting for the Recording feature. The Recording feature enables users to record audio and web collaboration sessions. When the Recording feature is enabled for the system, you can then enable the Recording feature on a per user basis.

### Procedure

1. In the Provisioning Client window, select **System Management > System Default Settings**.
2. On the System Default Settings tab, select (check) the **Allow recording** check box.
3. Click **Save**.

**Related links**

Both deployments on page 347

## Configuring the recording feature for users

You can configure a single user at one time or you can configure multiple users at one time. In a typical deployment scenario, it is likely that you will enable recording for configure multiple users at one time.

**Related links**

Both deployments on page 347

Modifying a single user on page 349

Modifying multiple users at one time on page 235

## Modifying a single user

### Before you begin

You must be logged into Provisioning Client.

### About this task

Use this procedure to configure the Recording feature for a user.

**Note:**

If you want to configure the Recording feature for multiple users at one time, you can use the Bulk Provisioning feature (**User Management > Bulk Provisioning**) in Provisioning Client.

### Procedure

1. In the Provisioning Client window, select **User Management > Search Users**.
2. On the Advanced Search tab, click **Search** to view all provisioned users.
3. In the Login Name column, click on the Login Name of the user to whom you want to assign the Recording feature.
4. On the User page, click the **Actions** tab.
5. On the Actions tab, click **Conferencing**.
6. On the Conferencing User page, select (check) the **Enable Recording** check box.
7. Click **Save**.
8. Repeat Steps 2 through 7 for each user.

**Related links**

Configuring the recording feature for users on page 349

## Modifying multiple users at one time

### Before you begin

- You must be logged into Provisioning Client.

**Warning:**

If you have an Avaya Aura® deployment, any changes you make may cause the Provisioning Client data to become out of sync with the data in Avaya Aura System Manager. You should only modify data to fix sync issues that cannot be resolved from the System Manager interface.

### About this task

Use this procedure to modify the conference class of service, video (enable/disable) setting, and recording (enable/disable) setting for multiple users at one time (that is, bulk provisioning). In this procedure, you will identify the list of users you want to modify by specifying search criteria.

### Procedure

1. In the Provisioning Client window, select **User Management > Bulk Provisioning**.
2. From the Field box, select the user criterion you want to search.
3. From the Operation box, select the search operation you want to perform.
4. In the Value box, specify the appropriate search information for the users.

5. Click **Add Criteria**.

   **Note:**

   You can modify up to 1000 users at any one time.

6. Repeat Steps 2 through 5 to specify any other search criteria.
7. When finished specifying your search criteria, click **Search**.

   The users who match your search criteria are displayed.

   Alternatively, you can select all users.

8. Click the check box for each user you want to modify.
9. In the Actions area, select the check box for each setting you want to modify for all of the selected users, and then select the appropriate value. See Bulk Provisioning page field descriptions on page 236.
10. Click **Commit**.

**Related links**

Adding a user for Avaya Aura Conferencing (AAC) for Turnkey on page 228
Configuring the recording feature for users on page 349
Bulk Provisioning page field descriptions on page 236

## Bulk Provisioning page field descriptions

| Name | Description |
|---|---|
| **Field** | Displays the following fields to search in the user data:<br>• **Login Name**<br>• **Communication Address Handle**<br>• **Communication Address Domain**<br>• **Last Name**<br>• **First Name**<br>• **Profile name**<br>• **Directory Sync Status**: This field has the following options:<br>- **Pending (sync error or out of filter scope)**<br>- **Synced from directory**<br>- **Local user**<br>• **Created (yyyy-mm-dd hh:mm:ss)**<br>• **Video Enabled**<br>• **Recording Enabled** |

*Table continues…*

| Name | Description |
|---|---|
| | • **Video Class** |
| **Operation** | The particular list of operations depends on the field selected. For example, for text fields, the operations are:<br>• **Starts with**<br>• **Contains**<br>• **Equals**<br>• **After**<br>• **Before**<br>For boolean fields and for the **Directory Sync Status** field, you cannot change the operation. It is always **Equals**. For the **Created (yyyy-mm-dd hh:mm:ss)** field, the options are **After** or **Before**. |
| **Value** | Displays the data to find in the specified user field. |

| Button | Description |
|---|---|
| **Add Criteria** | Adds the information you specified in the **Field**, **Operation**, and **Value** fields into the search criteria list box. |
| **Edit** | Enables you to modify the selected search criteria. |
| **Remove** | Deletes the selected search criteria. |
| **Remove all** | Deletes all the search criteria. |
| **Search** | Searches the user data using the displayed search criteria. |
| **Commit** | Saves the changes. |
| **Export Search Results to CSV** | Exports the search results to a spreadsheet. |

| Name | Description |
|---|---|
| **Directory Distinguished Name column** | Displays an element which operates in conjunction with the search scope.<br>The element is a tree to synchronize users. The domain part of the distinguished name is automatically based on the selected domain and cannot be changed. For example, cn=Users,dc=example,dc=com display. |
| **Login name column** | Displays the login name of each user. |
| **Communication Profile** | Displays the administered communications profile for each user. |
| **Last Name** | Displays the last name of each user. |
| **First Name** | Displays the first name of each user. |

| Name | Description |
|---|---|
| **Conference Profile** | Specifies the conference class of service to assign to the selected users. |
| **Enable Video** | Specifies whether video is enabled or disabled for the selected users. |
| **Enable Recording** | Specifies whether the recording feature is enabled or disabled for the selected users. |
| **Delete User** | Specifies whether to delete all selected users. |

**Related links**

Modifying multiple users at one time on page 235

## Configuring the Recording backup server

### Before you begin

- The backup server must support the ssh protocol. In other words, it must be an SSH server.
- The backup server must support rsync.
- The backup server must support a regular bash, or CSH shell without specific programs that would impact rsync operations over the SSH or RSH.
- You must have a user login (for example, admin) that can access the backup server and has read and write permissions for the backup folder.

### About this task

Use this procedure to configure the server that will store backup files from the Recording server.

### Procedure

1. Log on to the primary media server in the cluster as `ntsysadm` through ssh or directly on the server console.
2. Enter **`su -`** to log on as root.
3. At the prompt `password`, type the root password, and press **Enter**.
4. Type `configRecordingBackup.pl -backupuser <`*`remote user ID`*`> -backupip <`*`IP address of backup server`*`>`, and press **Enter**.
5. To verify that the configuration was successfully, type `ssh -i /admin/recording/bkrstr-recording_id_rsa <`*`admin@remote server`*`>`, and press **Enter** .

   You should be logged on to the backup server without being prompted for a password.
6. Repeat steps 1–5 for each recording media server cluster.
7. In the navigation pane of Element Manager Console, click **Addresses**.
8. In the Addresses window, click **Add (+)**.

9. In the Add IPv4 Address dialog box, complete the following fields:
    - **Logical Name**: Type the logical name for the backup server.
    - **IPv4 Address**: Type the IP address for the backup server.
10. Click **Apply**.
11. In the navigation pane of Element Manager Console, select **External Nodes**.
12. In the External Nodes window, click **Add (+)**.
13. In the Add External Node dialog box, complete the following fields:
    - **Logical Name**: Type another logical name for the backup server.
    - **IPv4 Address**: Type the IP address for the backup server.
14. Click **Apply**.
15. In the navigation pane of Element Manager Console, select **Recording > Backup Locations**.
16. In the Add Backup Locations dialog box, complete the following fields:
    - **Name**: Type the name of the backup server.
    - **Node**: Select the node for the backup server.
    - **Path**: Type the absolute path under which recordings should be stored on the backup server.
17. Click **Apply**.
18. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > Recording > Backup/Purge Settings**.

    The Backup/Purge Settings dialog box appears. For more information, see Backup/Purge Settings dialog box field descriptions on page 355.
19. Modify the settings and click **OK**.

    **Note:**

    - The purge process always deletes the oldest records first. You can configure Avaya Aura® Conferencing to purge recordings when they exceed a certain size or when they exceed a certain date.
    - The timestamp is reset when recordings are restored to prevent the recordings from being immediately purged in the next purge process.
    - Changing the recording metadata (for example, by changing the title or by changing whether it is shared) will reset the backup flag and cause the file to be backed up again.
20. In the navigation pane of Element Manager Console, select **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > Recording > Purge Thresholds**.

For more information, see Purge Thresholds dialog box field descriptions on page 356.

21. In the Purge Thresholds dialog box, configure the thresholds at which an alarm will be triggered for disk space usage on the Recording media server recordings partition. Using the **Major Threshold** box and the **Critical Threshold** box, you can set thresholds for major and critical alarms. Once a critical threshold is crossed, the purge job will start deleting the oldest recordings until disk space is freed at or below the value specified in the **Retain** box.
22. When finished, click **OK**.

**Related links**

Both deployments on page 347
Backup/Purge Settings dialog box field descriptions on page 355
Purge Thresholds dialog box field descriptions on page 356

## Backup/Purge Settings dialog box field descriptions

| Name | Description |
|---|---|
| Schedule | Specify whether you want to schedule a backup and/or purge to be performed every day at a specific time.<br>To schedule a daily backup and/or purge, click **Daily**, and specify the hour and minute (in 24-hour format) at which you want the backup and/or purge to be performed. |
| Actions | Click the check box of the process you want to schedule. If you want to schedule both a backup and a purge, select both the **Backup** check box and the **Purge** check box. If both the **Backup** check box and the **Purge** check box are checked, the purge process will delete only the recordings that have been backed up. If only the **Purge** check box is checked, the purge process will delete all recordings regardless of whether the recordings are backed up.<br>If you want to trigger a purge based on a maximum retention period, specify the number of days for which you wish to retain the recording file in the **Max days** field. You can specify an amount between 0 and 999. By default, **Max days** is set to 0. When **Max days** is set to 0, a maximum retention period is not used. Instead, a purge is triggered when the disk usage exceeds a critical threshold and continues deleting recordings until a retain threshold is reached. You can configure these thresholds.<br>**Note:**<br>• The purge process always deletes the oldest records first.<br>• The timestamp is reset when recordings are restored to prevent the recordings from being immediately purged in the next purge process.<br>• Changing the recording metadata (for example, by changing the title or by changing whether it is shared) will reset the backup flag and cause the file to be backed up again. |
| Location | Select the appropriate backup location. |

**Related links**

Configuring the Recording backup server on page 353

## Purge Thresholds dialog box field descriptions

| Name | Description |
|---|---|
| Retain | Once a critical threshold is crossed, the purge job (if enabled) will start deleting the oldest recordings until disk space is freed at or below the Retain value you specify. |
| Major Threshold | Configure the threshold at which a major alarm will be triggered for disk space usage on the Recording media server recordings partition. |
| Critical Threshold | Configure the threshold at which a critical alarm will be triggered for disk space usage on the Recording media server recordings partition. |

**Related links**

Configuring the Recording backup server on page 353

# Configuring codecs for recording

In Avaya Aura® Conferencing, the recording function operates by establishing a trunk between the conferencing media server and the recording media server. You can specify the audio codec for this trunk.

**Related links**

Both deployments on page 347

Configuring the codecs for the recording trunks on page 356

Recording functionality and the upgrade process on page 357

## Configuring the codecs for the recording trunks

This audio codec setting is a global setting which will apply to all recording media servers in your deployment. The highest selected codec is used as long as both the recording and conferencing media servers are capable of using it, even if it is disabled in the media server configuration.

### About this task

Use this task to specify a G.711, G.722, or G.726 audio codec for the recording trunks in your deployment.

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Recording Trunk Codec Settings**.
2. On the **Recording Trunk Codec Settings** dialog, re-order the list of audio codecs in accordance with your preferences.
3. Click **Ok**.

**Related links**

[Configuring codecs for recording](#) on page 356
[Recording Trunk Codec Settings field descriptions](#) on page 357

### Recording Trunk Codec Settings field descriptions

| Name | Description |
|---|---|
| **Enabled** | The Enabled panel lists the audio codecs that are available. You can select each item in this list. |

| Button | Description |
|---|---|
| **Up** | Moves the selected audio codec to a higher location on the list. |
| **Down** | Moves the selected audio codec to a lower location on the list. |
| **Ok** | Click **Ok** to apply your changes. |
| **Cancel** | Click **Cancel** to disregard your changes. |

**Related links**

[Configuring the codecs for the recording trunks](#) on page 356

## Recording functionality and the upgrade process

When you upgrade from older Avaya Aura® Conferencing releases to the new Avaya Aura® Conferencing release, all your existing recordings are saved and you can play them on the new player after the upgrade. Re-encoding of existing recordings is not necessary when you upgrade from older Avaya Aura® Conferencing releases to the new Avaya Aura® Conferencing release. The existing recordings are compatible with the new player. You can backup or delete any existing recordings. Similarly, you can restore any existing backups.

In this release of Avaya Aura® Conferencing, you can specify the audio codecs to use for the trunk that Avaya Aura® Conferencing establishes between the conferencing media server and the recording media server. In previous releases of Avaya Aura® Conferencing, you could not specify this audio codec. During the upgrade process from older Avaya Aura® Conferencing releases to the new Avaya Aura® Conferencing release, Avaya Aura® Conferencing sets the preference order for the audio codecs to:

1. G.722 (most preferred)
2. G.711
3. G.726 (least preferred)

**Related links**

[Configuring codecs for recording](#) on page 356

## Web Conferencing Server (WCS) clusters

Within the Avaya Aura® Conferencing environment, the concept of a ‘cluster’ provides a mechanism for Avaya Aura® Conferencing administrators to provision a collection of servers as one single server. This mechanism reduces the number of configuration tasks but also maximizes load balancing between the servers. In this release, Avaya Aura® Conferencing supports the concept of a media server (MS) cluster and a Web Conferencing Server (WCS) cluster. In this Avaya Aura® Conferencing release, WCS clusters replace WCS groups from previous releases.

When Avaya Aura® Conferencing chooses which WCS cluster to use for a particular conference, it uses the following process:

- Avaya Aura® Conferencing checks if there is a WCS cluster provisioned to serve the user (conference owner) in their location.
- If there are no WCS clusters available in the same location as the user, Avaya Aura® Conferencing searches for WCS clusters serving the user’s location, and selects the least loaded WCS from amongst those clusters.
- If there are still no WCS available, Avaya Aura® Conferencing uses the default WCS cluster.

There are additional options available if you wish to ensure that users from a particular location use the system resources in another location.

Avaya Aura® Conferencing follows this process:

- When it chooses which WCS to use for hosting a conference.
- When it chooses which WCS to use for recording a conference.
- When it chooses which WCS to use for playing back a conference.
- When it chooses which WCS to use for encoding a conference that does not include web collaboration.

Encoding, within this context, refers to the process of processing a conference recording to convert it to a playable format. If the conference contains web collaboration, Avaya Aura® Conferencing uses the hosting server for the encoding process.

You must also provision dedicated WCS clusters if you wish to support event conferences. For more information about event conferences, see Event conferencing and media cascading on page 45.

**Related links**

WCS clusters and the upgrade process on page 250
WCS clusters and Application Delivery Controller (ADC) functionality on page 250
Creating a new WCS cluster on page 250
Configuring the default cluster on page 251
Assigning WCS clusters to serving locations on page 252
Assigning WCS clusters to physical locations on page 253
Assigning WCS clusters to hosting locations on page 255
Configuring WCS clusters for event conferences on page 256
Both deployments on page 347

# Chapter 22: Configuring load balancing

## Load-balancing functionality

For Avaya Aura® Conferencing, load-balancing is supported through the use of more than one server for a particular purpose. For example, you could have more than one Web Conferencing Server (WCS) or you could have more than one Document Conversion Server (DCS) or you could have more than one media server. The WCS hosts web conferences. The DCS converts files for sharing online. The media server provides a number of functions, such as, audio/video mixing, Dual Tone Multi Frequency (DTMF) detection, and message playing. In times of heavy system usage, a single WCS might become overloaded. Similarly, if large numbers of users are converting files at the same time, a single DCS might reach capacity. The same is true for a single media server. For these situations, it is a good idea to share the load across multiple WCSs or multiple DCSs or multiple media servers. If the first server is full, the traffic can automatically go to another available server.

### WCS

For the WCS, Avaya Aura® Conferencing uses the concept of WCS clusters. Clusters are groups of WCSs and these groups are assigned to a location. For more information about WCS clusters, see WCS Clusters on page 249.

### DCS

For the DCS, Avaya Aura® Conferencing , uses the concept of multiple DCSs and a performance load factor. Avaya Aura® Conferencing distributes conversion requests between multiple DCSs based on the load on each DCS in such as way as to minimize the conversion time. For more information about load balancing for the DCS, see Multiple Document Conversion Servers (DCSs) on page 275.

Redundancy of the DCS is also supported through the provision of multiple DCSs. So, if a DCS fails, the load is switched to another DCS. For more information, see Example scenarios on page 360.

### Media servers

For media servers, Avaya Aura® Conferencing uses the concept of media server clusters. Clusters are groups of media servers and these groups are assigned to a location.

Media cascading reduces the number of media streams travelling across the WAN by consolidating these streams based by location. This technique is applied to both audio and video streams. Media cascading provides bandwidth optimization with no significant reductions in the quality of audio or video. Conferences are scalable with proper configuration and management which is fully transparent to end users. For more information about media server clusters, see Software installation procedure for adding additional media servers on page 118.

# Chapter 23: Configuring Automatic Disaster Recovery (ADR)

## Example scenarios

You can configure ADR in either automatic failover or manual failover mode. In both modes, the secondary Avaya Aura® Conferencing system detects a failure on the primary Avaya Aura® Conferencing system once the detection time interval has been exceeded. In automatic failover mode, the secondary Avaya Aura® Conferencing system transitions from standby to active. In manual failover mode, the secondary Avaya Aura® Conferencing system detects the failure, raises an alarm, but does not transition from standby to active. You must manually intervene to switch the secondary Avaya Aura® Conferencing system from standby to active.

These example scenarios assume that before the disaster, the primary Avaya Aura® Conferencing system is in an active (unlocked) state and the secondary Avaya Aura® Conferencing system is in a standby (locked) state.

### Example of a failover

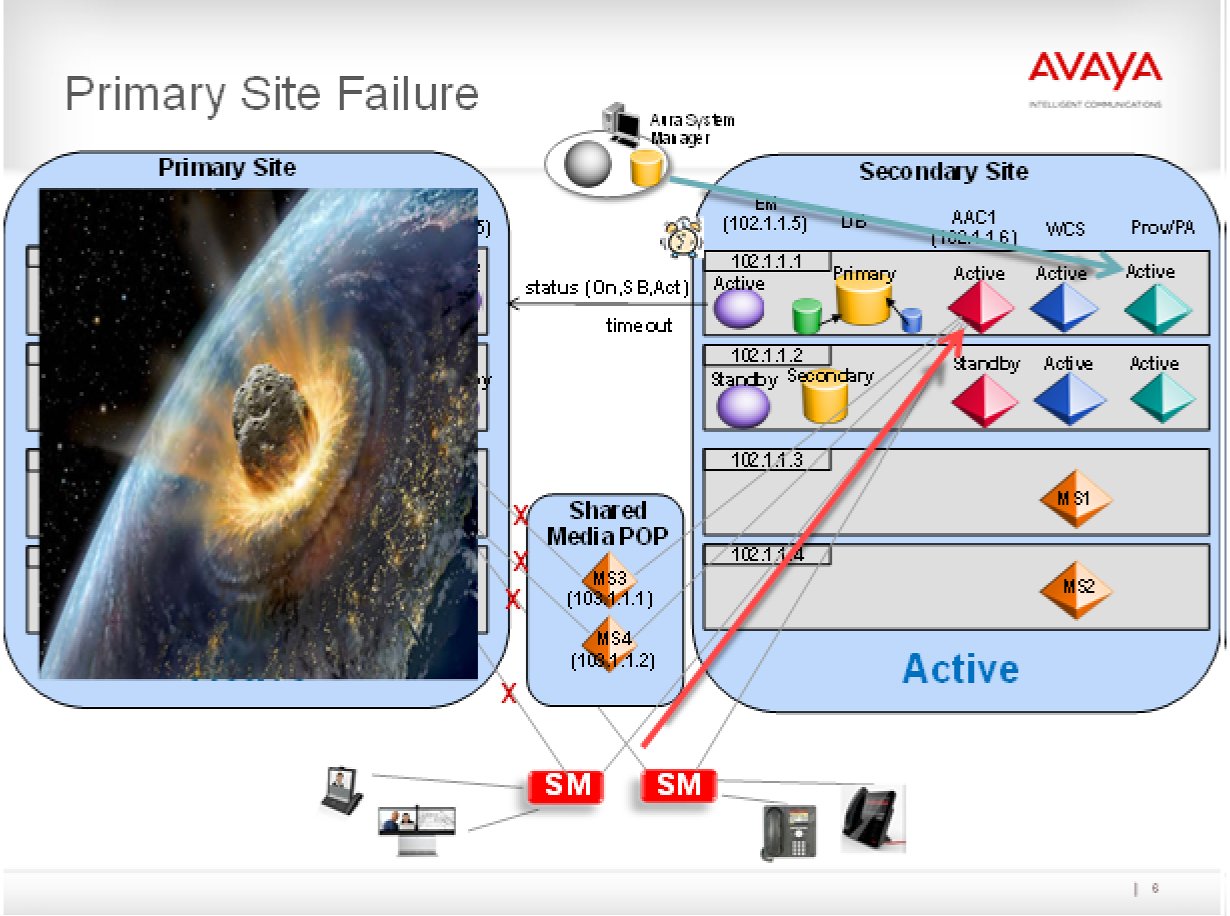


**Figure 21: An example of a failure of the primary site**

**Related links**

Automatic failover scenarios on page 361
Manual failover on page 362

## Automatic failover scenarios

### The primary Avaya Aura® Conferencing system fails due to a real disaster at the primary site

1. Once the detection time interval has been exceeded, the secondary Avaya Aura® Conferencing system detects the failure at the primary Avaya Aura® Conferencing site.
2. The secondary Avaya Aura® Conferencing system transitions to an operational system service state of Active (Unlocked).

### The primary Avaya Aura® Conferencing system fails due to a temporary power outage at the primary site

1. Once the detection time interval has been exceeded, the secondary Avaya Aura® Conferencing system detects the failure at the primary Avaya Aura® Conferencing site.
2. The secondary Avaya Aura® Conferencing system transitions to an operational system service state of Active (Unlocked).
3. The power returns to the primary site.
4. The primary and secondary Avaya Aura® Conferencing systems establish detection communications.
5. The primary Avaya Aura® Conferencing system transitions to an operational system service state of Active (Unlocked).

### The primary and secondary Avaya Aura® Conferencing systems loose their network connection

1. Connections between the primary and secondary Avaya Aura® Conferencing systems are lost for a period that is greater than the detection time interval.
2. The primary Avaya Aura® Conferencing system assumes that there is a failure on the secondary Avaya Aura® Conferencing system and remains in an operational system service state of Active (Unlocked).
3. The secondary Avaya Aura® Conferencing system assumes that there is a failure on the primary Avaya Aura® Conferencing system and transitions to an operational system service state of Active (Unlocked).
4. At this point, call traffic is potentially split between both systems. Avaya Aura® Conferencing will always attempt to route to the primary system. If the primary system is responding to the SIP pings, then it will receive the traffic.
5. The network outage is resolved and connectivity is restored.
6. The primary and secondary Avaya Aura® Conferencing systems establish detection communications.
7. The secondary Avaya Aura® Conferencing system remains in a system service state of Active (Unlocked).
8. The primary Avaya Aura® Conferencing system transitions to an operational system service state of Standby (Locked).

**Related links**

Example scenarios on page 360

## Manual failover

### The primary Avaya Aura® Conferencing system fails due to a real disaster at the primary site

1. Once the detection time interval has been exceeded, the secondary Avaya Aura® Conferencing system detects the failure at the primary Avaya Aura® Conferencing site.

2. The secondary Avaya Aura® Conferencing system raises an alarm to indicate that the primary system is unreachable.
3. You must log into the secondary Avaya Aura® Conferencing system and change the operational system service state to Active (Unlocked).

### The primary Avaya Aura® Conferencing system fails due to a temporary power outage at the primary site

1. Once the detection time interval has been exceeded, the secondary Avaya Aura® Conferencing system detects the failure at the primary Avaya Aura® Conferencing site.
2. The secondary Avaya Aura® Conferencing system raises an alarm to indicate that the primary system is unreachable.
3. You must log into the secondary Avaya Aura® Conferencing system and change the operational system service state to Active (Unlocked).
4. The power returns to the primary site.
5. The primary and secondary Avaya Aura® Conferencing systems establish detection communications.
6. The primary Avaya Aura® Conferencing system transitions to an operational system service state of Standby (Locked).

### The primary and secondary Avaya Aura® Conferencing systems loose their network connection and you do not manually intervene to change the system service state to Active (Unlocked) on the secondary Avaya Aura® Conferencing system

1. Connections between the primary and secondary Avaya Aura® Conferencing systems are lost for a period that is greater than the detection time interval.
2. The primary Avaya Aura® Conferencing system assumes that there is a failure on the secondary Avaya Aura® Conferencing system and remains in an operational system service state of Active (Unlocked).
3. The secondary Avaya Aura® Conferencing system assumes that there is a failure on the primary Avaya Aura® Conferencing system and raises an alarm to indicate that the primary system is unreachable.
4. At this point, you can verify that the failure does not exist on the primary system and so you can leave the secondary Avaya Aura® Conferencing system in an operational system service state of Standby (Locked).
5. The network outage is resolved and connectivity is restored.
6. The primary and secondary Avaya Aura® Conferencing systems establish detection communications.
7. The primary Avaya Aura® Conferencing system remains in a system service state of Active (Unlocked).
8. The secondary Avaya Aura® Conferencing system remains in a system service state of Standby (Locked).

### The primary and secondary Avaya Aura® Conferencing systems loose their network connection and you manually intervene to change the system service state to Active (Unlocked) on the secondary Avaya Aura® Conferencing system

1. Connections between the primary and secondary Avaya Aura® Conferencing systems are lost for a period that is greater than the detection time interval.
2. The primary Avaya Aura® Conferencing system assumes that there is a failure on the secondary Avaya Aura® Conferencing system and remains in an operational system service state of Active (Unlocked).
3. The secondary Avaya Aura® Conferencing system assumes that there is a failure on the primary Avaya Aura® Conferencing system and raises an alarm to indicate that the primary system is unreachable.
4. At this point, you do not verify that the primary system is operational and you log into the secondary Avaya Aura® Conferencing system and change the operational system service state to Active (Unlocked).
5. The network outage is resolved and connectivity is restored.
6. The primary and secondary Avaya Aura® Conferencing systems establish detection communications.
7. The primary Avaya Aura® Conferencing system transitions to an operational system service state of Standby (Locked).
8. The secondary Avaya Aura® Conferencing system remains in a system service state of Active (Unlocked).

**Related links**

Example scenarios on page 360

## Data synchronization

Once you configure ADR, the process of data synchronization begins. Avaya Aura® Conferencing uses a script called dbBackupForADR.pl to ensure that the secondary system contains the latest information from the primary system. For each cycle of data synchronization, the latest database information from the primary system replaces the existing database information on the secondary system.

It is important to note that there are routine situations in which data synchronization is not successful. For example, data synchronization is not successful if the primary or secondary systems are currently being upgraded. Data synchronization is not successful if the previous data synchronization cycle is still running on the secondary Avaya Aura® Conferencing system.

The data synchronization occurs at intervals. This pattern of periodic synchronization cycles means that the updates which occur on the primary Avaya Aura® Conferencing system during the interval are not available on the secondary Avaya Aura® Conferencing system.

For a simple restoration of a primary Avaya Aura® Conferencing system, in cases where you have not reconfigured the secondary servers on System Manager, you can use the latest database information from the primary site. This is the file that dbBackupForADR.pl produced. You should use this file in preference to the daily scheduled database backup, because dbBackupForADR.pl executes several times a day and is likely to be a more recent file.

During the database synchronization process, Avaya Aura® Conferencing generates a number of alarms (approximately 20 alarms). These alarms are normal and will clear when the database synchronization process finishes.

## Checklist for installing and configuring Automatic Disaster Recovery (ADR)

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Understand how ADR operates. | • Example scenarios on page 360<br>• Automatic failover on page 361<br>• Manual failover on page 362<br>• Data synchronization on page 364<br>• Upgrades and ADR on page 381<br>• Limitations of ADR on page 391 | | |
| 2 | Install the primary system. | Installing or upgrading a primary system on page 366 | | |
| 3 | Install the secondary system. | Installing or upgrading a secondary system on page 367 | | |
| 4 | Install the MCP load and database software. | Installing the MCP load and database software on page 368 | **Note:**<br>In a redundant system, with automatic disaster recovery (ADR), the System Manager and Session Manager addresses should be the same. | |

*Table continues…*

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 5 | Update Element Manager on the secondary system. | Updating Element Manager on the secondary system on page 369 | | |
| 6 | Create a SIP entity between the Session Manager (or your PBX equivalent) and the application server in the secondary system. | Configuring the route to Avaya Aura® Conferencing on System Manager on page 309 | You require SIP entity, entity link, and a routing policy for each site. | |
| 7 | Configure the routing policies on both systems. | Configuring the routing policies on page 370 | | |
| 8 | Configure ADR on the primary system. | Configuring ADR on the primary system on page 372 | | |
| 9 | Configure ADR on the secondary system. | Configuring ADR on the secondary system on page 374 | | |
| 10 | Complete the installation on both the primary and secondary systems. | Completing the installation on both systems on page 380 | | |

# Installing a primary system

## About this task

Use this task to install or upgrade the primary system and to take a backup of the primary system database.

- The physical site to which a given server belongs determines if the network element instances on it are considered as shared with the secondary system. Any network element instance that is configured to belong to a server that is in the same physical site as the primary system Element Manager is treated as a unique to the primary system during the initial deployment of the secondary system. All network elements instances that are configured to belong to servers in other physical sites are treated as shared between the two systems.
- Do not configure the address of the peer secondary system yet. If you configure it now, the resulting backup will not be available for use to create the secondary system.

## Procedure

1. Install the Avaya Aura® Conferencing platform on the primary site.

   For more information, see Installing the AAC Platform on page 121.

2. Install the Avaya Aura® Conferencing components on the primary site.

   For more information, see Installing the components for Avaya Aura® Conferencing for Aura on page 132 or Installing the components for Avaya Aura® Conferencing for Turnkey on page 141.

3. Backup the database of the primary system by logging in to the primary database of the primary system as the `ntdbadm` user.
4. Enter the following command: `cd /var/mcp/run/MCP_18.X/mcpdb_0/bin/util`.
5. Enter the following command: `./dbBackup.pl dbBkupForSecondarySystem`.

### Next steps

You must set up and configure the entire system before commencing with Installing a secondary system on page 367.

## Installing a secondary system

### Before you begin

Complete the steps in Installing a primary system on page 366.

### About this task

Use this task to install or upgrade the secondary system to support ADR.

**Note:**

If your deployment uses virtual servers by way of VMware software, you must use the platform OVA for the secondary system. Do not use the medium simplex or medium redundant OVAs.

### Procedure

1. Install the Avaya Aura® Conferencing platform on the secondary site, using the `mcpADRInstaller`, instead of the `mcpInstaller`.

   For more information, see Installing the AAC Platform on page 121.

   In addition, if the primary system has a patch installed on it, you must also install this patch on the secondary system. For more information about installing patches, features packs, and service packs, see *Upgrading Avaya Aura® Conferencing*, which is available on https://support.avaya.com/.

2. Install the Avaya Aura® Conferencing components on the secondary site.

   For more information, see Installing the components for Avaya Aura® Conferencing for Aura on page 132 or Installing the components for Avaya Aura® Conferencing for Turnkey on page 141.

   During the installation, at the prompt for the Element Manager password, enter the same password as the Element Manager administrator password in the primary system.

3. Update Element Manager on the secondary system.

   For more information, see Updating Element Manager on the secondary system on page 369.

4. Configure ADR on the secondary system, as was described for the primary system in Installing or upgrading a primary system on page 366.

### Next steps

Proceed to Completing the installation on both systems on page 380.

**Related links**

Installing the MCP load and database software on page 368
Updating Element Manager on the secondary system on page 369

## Installing the MCP load and database software

The `mcpADRInstaller.pl` script is similar to the `mcpInstaller.pl` script and performs many operations automatically. However, if some files or data are not available from the primary system, then you must manually install the Avaya Aura® Media Server (MS) platform on the secondary Element Manager server after the script completes.

**Note:**

During the database synchronization process, Avaya Aura® Conferencing generates a number of alarms (approximately 20 alarms). These alarms are normal and will clear when the database synchronization process finishes.

### About this task

Use this task to install the MCP load and database software.

### Procedure

1. Log in to the secondary system Element Manager server as the `ntappadm` user.
2. Copy the MCP_18.X core application bundle to the `/var/mcp/extract` directory using FTP.
3. Run the `mcpADRInstaller.pl` command.

   The `mcpInstaller.pl` and `ADRmcpInstaller.pl` scripts automatically install the Avaya Aura® Media Server (MS) on the Element Manager server, as appropriate.

### Next steps

Refer back to Installing a secondary system on page 367 to see the next step.

**Related links**

Installing a secondary system on page 367

# Updating Element Manager on the secondary system

## About this task

Use this task to update hostnames in Element Manager on the secondary system. The mcpInstaller.pl and ADRmcpInstaller.pl scripts automatically configure certificates for all network elements but it is a good idea to verify the certificates.

## Procedure

1. Login to the Element Manager console on the secondary system and perform the following updates:

    a. Verify the HTTPS certificates (restored from the primary system) and ensure that the certificates are correctly set up for the secondary system. The mcpInstaller.pl and ADRmcpInstaller.pl scripts automatically configure certificates for all network elements. For more information, see Guidelines for certificate configuration on page 566.

    b. Verify the list of IP addresses for the secondary system.

    - On the Element Manager console, select **Addresses**.
    - Verify the IP addresses and correct any errors before deploying and starting the network elements. It is important to verify the list carefully.
    - Close the **Addresses** dialog.

2. Deploy and start all of the network element instances that are unique to the secondary system.

    For more information, see Deploying a Network Element instance on page 244 and Starting a network element instance on page 669.

    Do not attempt to deploy and start any shared network element instances from the secondary system while the primary system is active.

3. Manually disable the features that are not required on the secondary system.

    For example, manually disable recording for the media server clusters in the secondary system. For more information, see Creating a new media server cluster on page 245 and Configuring the Recording feature on page 339.

## Next steps

Refer back to Installing or upgrading a secondary system on page 367 to see the next step.

### Related links

Installing a secondary system on page 367

# Configuring the routing policies for ADR

You require a SIP entity, entity link, and routing policy for each site. For each the routing policies, you must allocate a rank.

### Before you begin

Before you configure the routing policies for ADR, you must:

- Configure domains and locations.
- Configure SIP Entities for the primary and secondary systems.
- Configure Entity Links for the primary and secondary systems.
- Configure dial patterns.

The System Manager documentation describes each of these tasks and is available from the Avaya Support website: http://support.avaya.com.

### About this task

Use this task to apply the correct ranking to routing policies on the primary and secondary systems.

### Procedure

1. Log in to System Manager.
2. On the System Manager console, click **Elements** > **Routing**.
3. Configure time ranges.
    a. Click **New**.
    b. Enter a name of 24/7.
    c. Select all 7 days.
    d. Enter a start time of 00:00.
    e. Enter an end time of 23:59.
    f. Click **Commit**.
4. Ensure that you have completed the pre-requisites:
    - Configure domains and locations.
    - Configure SIP Entities for the primary and secondary systems.
    - Configure Entity Links for the primary and secondary systems.
    - Configure dial patterns.
5. Configure the routing policy for the primary system.
    a. Click **New**, to display the panel to add a routing policy.
    b. Enter the name of the routing policy for the primary site.
    c. Click **Select** under **SIP Entity as Destination**.

d. In the **SIP Entities** panel, select the entry which has the application server service address of the primary system.

e. Click **Select** at the bottom of the **SIP Entities** panel.

f. Add the **24/7** time range in the **Time of Day** section.

g. Set the ranking to **0**.

The ranking value indicates the routing policy priority. A lower ranking value indicates a higher priority.

h. Add the dial patterns that you configured as part of the pre-requisites.

i. Click **Commit**

6. Configure the routing policy for the secondary system.

a. Click **New**, to display the panel to add a routing policy.

b. Enter the name of the routing policy for the primary site.

c. Click **Select** under **SIP Entity as Destination**.

d. In the **SIP Entities** panel, select the entry which has the application server service address of the secondary system.

e. Click **Select** at the bottom of the **SIP Entities** panel.

f. Add the **24/7** time range in the **Time of Day** section.

g. Set the ranking to **1**.

The ranking value indicates the routing policy priority. A lower ranking value indicates a higher priority.

h. Add the dial patterns that you configured as part of the pre-requisites.

i. Click **Commit**

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

# Configuring ADR

There are a number of tasks involved in the configuration of ADR. You must install and configure a secondary Avaya Aura® Conferencing system. You must add this secondary system to the Element Manager Console. You must also add this secondary system to an ADR configuration.

The steps in this section show an example configuration — ADR in an Automatic Failover Mode with a Peer Failure Detection Period of 3 minutes. If you require different settings, simply substitute your required values in the procedures in this section. The values for Failover Mode and Peer Failure Detection Timeout must be the same on both the primary and secondary systems. In other words, both systems must be set to manual or auto Failover Mode and the Peer Failure Detection Period must be identical as well.

Before you begin to configure ADR, you must have the following information for both systems:

- EMIntOAMSvcAddr of the secondary system
- EMIntOAMSvcAddr of the primary system

**Related links**

Configuring ADR on the primary system on page 372
Configuring ADR on the secondary system on page 374
Performing maintenance tasks on your ADR configuration on page 376
Bulk configuration utility on page 377

## Configuring ADR on the primary system

### Before you begin

Make a note of:

- EMIntOAMSvcAddr of the secondary system
- EMIntOAMSvcAddr of the primary system

### About this task

Use this task to configure automatic disaster recovery on the primary system.

### Procedure

1. Login to the Element Manager Console of the primary system.
2. Select **Addresses** and click **Add (+)**.
3. In the **Add IPv4 Address** dialog, configure the following values:

| Field | Value |
|---|---|
| **Logical Name** | SysBIntOAMSvcAddr |
| **IPv4 Address** | *<EMIntOAMSvcAddr of the secondary system>* |

4. Click **Apply**.
5. Close the **Addresses** dialog.
6. Navigate to **Automated Disaster Recovery** > **ADR Configuration**.
7. On the **ADR Configuration** dialog, click **Add (+)**.
8. In the **Add Automated Disaster Recovery Configuration** dialog, configure the following values:

| Field | Value |
|---|---|
| **Role** | Primary |

| Field | Value |
|---|---|
| **Failover Mode** | Auto |
| **Peer Address** | SysBIntOAMSvcAddr |
| **Peer Failure Detection Period** | 3 |

9. Click **Apply**.
10. Close the **ADR Configuration** dialog.

    **Note:**

    If this system has shared media servers — in other words, media servers at points of presence which are used by both ADR systems — then the secondary system must be configured on the primary system. This ensures that the shared media servers can accept traffic from the application servers defined in the secondary system in the event of a failover occuring.

11. Add the IP address for the secondary system application server.
    1. Select **Addresses** and click **Add (+)**.
    2. In the **Add IPv4 Address** dialog, configure the following values:
       - Set the **Logical Name** to `SysBAS1OAMSvcAddr`.
       - Set the **IPv4 Address** to *`<AS1IntOAMSvcAddr of the secondary system>`*
    3. Click **Apply**.
    4. Close the **Addresses** dialog.
12. Configure the secondary system application server:
    1. Navigate to **Automated Disaster Recovery** > **Secondary System Application Servers**.
    2. On the **Secondary System Application Servers** dialog, click **Add (+)**.
    3. In the **Add External Application Server** dialog, configure the following values:
       - Set **Name** to `SysBAppSvr1`.
       - Set **IPv4 Address** to `SysBAS1OAMSvcAddr`.
    4. Click **Apply**.
13. Close the **Secondary System Application Servers** dialog.

### Next steps

Proceed to Configuring ADR on the secondary system on page 374.

### Related links

Configuring ADR on page 371
Add External Application Server field descriptions on page 374

## Add External Application Server field descriptions

| Name | Description |
|---|---|
| **Name** | Enter a name for the secondary Avaya Aura® Conferencing system. |
| **IPv4 Address** | Select a server from the list of previously added servers. |

| Button | Description |
|---|---|
| **Apply** | Click **Apply** to save your changes. |
| **Cancel** | Click **Cancel** to clear your changes. |

**Related links**

Configuring ADR on the primary system on page 372

# Configuring ADR on the secondary system

### Before you begin

Configure the primary system. For more information, see Configuring ADR on the primary system on page 372.

### About this task

Use this task to configure automatic disaster recovery on the secondary system.

### Procedure

1. Login to the Element Manager Console of the secondary system.
2. Select **Addresses** and click **Add (+)**.
3. In the **Add IPv4 Address** dialog, configure the following values:

| Field | Value |
|---|---|
| **Logical Name** | SysAIntOAMSvcAddr |
| **IPv4 Address** | *<EMIntOAMSvcAddr of the primary system>* |

4. Click **Apply**.
5. Close the **Addresses** dialog.
6. Navigate to **Automated Disaster Recovery** > **ADR Configuration**.
7. On the **ADR Configuration** dialog, click **Add (+)**.
8. In the **Add Automated Disaster Recovery Configuration** dialog, configure the following values:

| Field | Value |
|---|---|
| **Role** | Secondary |

| Field | Value |
|---|---|
| **Failover Mode** | Auto |
| **Peer Address** | SysAIntOAMSvcAddr |
| **Peer Failure Detection Period** | 3 |

9. Click **Apply**.
10. Close the **ADR Configuration** dialog.

**Related links**

Configuring ADR on page 371
ADR Configuration dialog field descriptions on page 375

## ADR Configuration dialog field descriptions

| Name | Description |
|---|---|
| **Role** | Displays a list of roles.<br>**Primary** refers to the main or "master" configuration.<br>**Secondary** refers to the backup configuration which comes into operation in the event of a failure on the primary system. |
| **Failover Mode** | Displays a list of types of failover.<br>**Auto** refers to an automatic form of failover that requires little manual intervention.<br>**Manual** refers to a more basic form of failover that requires human intervention. |
| **Peer Address** | Displays a list of configured servers. Select a server to act as a secondary (backup) server and to which Avaya Aura® Conferencing will switch operations in the event of a failure on the primary (main) server. |
| **Peer Failure Detection Period** | Enter a time interval. If the primary system is inactive (offline) for this time interval, Avaya Aura® Conferencing initiates the ADR functionality. |

| Button | Description |
|---|---|
| **Apply** | Click **Apply** to save your changes. |
| **Cancel** | Click **Cancel** to clear your changes. |

**Related links**

Configuring ADR on the secondary system on page 374

## Performing maintenance tasks on your ADR configuration

In terms of maintenance tasks, you can start or stop a primary or secondary system. You can change the service state. You can perform a manual synchronization.

### About this task

Use this task to perform simple maintenance on your system.

### Procedure

1. In the navigation pane of Element Manager Console, select **Automated Disaster Recovery** > **ADR Maintenance**.
2. On the **ADR Maintenance** dialog, .
3. Using the buttons, perform one of the following:

   Start

   Stop

   Lock

   Unlock

**Related links**

Configuring ADR on page 371
ADR Maintenance dialog field descriptions on page 376

## ADR Maintenance dialog field descriptions

| Name | Description |
|---|---|
| **Role** | Displays a list of roles.<br>**Primary** refers to the main or “master” configuration.<br>**Secondary** refers to the backup configuration which comes into operation in the event of a failure on the primary system. |
| **Failover Mode** | Displays a list of types of failover.<br>**Auto** refers to an automatic form of failover that requires little manual intervention.<br>**Manual** refers to a more basic form of failover that requires human intervention. |
| **Administrative** | Displays whether this system is enabled. |
| **Operational** | Displays whether this is a primary system (active) or a secondary system (standby). |

*Table continues…*

| Name | Description |
|---|---|
| **Peer Operational** | Displays whether the system can detect the other system. For example, it displays whether the primary system can detect the secondary system. |
| **Current State** | Displays the current state of the system. There are several possible states. For example, `waiting for next sync`. |
| **Last successful sync time** | Displays the time of the last successful synchronization. |
| **Next scheduled sync time** | Displays the time of the next planned synchronization. |

| Icon | Name | Description |
|---|---|---|
| 🟢 | Start | Click to start a system. |
| 🔴 | Stop | Click to stop a system. |
| 🔓 | Go Active (unlock) | Click to unlock a system. |
| 🔒 | Go Standby (unlock) | Click to lock a system. |
| 🛢 | Start manual sync | Click to start a manual (unscheduled) synchronization.. |

### Related links

Performing maintenance tasks on your ADR configuration on page 376

## Bulk configuration utility

Many customers have several instances of certain servers. For example, customers can install several media servers in order to provide additional conferencing capacity. This architecture is particularly common in the case of large deployments of Avaya Aura® Conferencing. In an ADR configuration, these customers may wish to share the media servers in the primary and secondary systems, rather than install and configure separate servers in the secondary system, which would incur additional costs.

In a scenario in which you wish to switch operations from the primary system to the secondary system, you can use a bulk configuration utility to simplify the process of engaging the shared network element instances on the secondary system. The converse is also true: You can use the bulk configuration utility to simplify the process of re-engaging the shared network element instances on the primary system.

Using the bulk configuration utility, you can create an ordered sequence of adoption for the shared servers. The bulk configuration utility enables you to group the shared servers and switch activity to them in a single action. This utility simplifies the process of switching activity from primary system to secondary system and from secondary system to primary system.

If none of the network element instances are shared between the primary and secondary systems, you do not require this utility because you can simply switch activity using the ADR Maintenance dialog. If some of the network element instances are shared, you can use this utility when you are manually switching activity between systems. It enables you to control the switching process and to schedule the switching of individual servers to ensure that there is no loss of service.

An individual bulk configuration is not shared between the primary and secondary servers. So, you must create a bulk configuration on the primary system for a switch from a primary system to a secondary system. You must also create a bulk configuration on the secondary system for a switch from a secondary system to a primary system.

**Related links**

Configuring ADR on page 371
Adding a bulk configuration on page 378
Editing a bulk configuration on page 379
Deleting a bulk configuration on page 379
Using the bulk configuration utility on page 380

## Adding a bulk configuration

### About this task

Use this task to create a bulk configuration.

### Procedure

1. Login to the Element Manager Console on the primary system or the secondary system.

   An individual bulk configuration is not shared between the primary and secondary servers. So, you must create a bulk configuration on the primary system for a switch from a primary system to a secondary system. You must also create a bulk configuration on the secondary system for a switch from a secondary system to a primary system.

2. Navigate to **Automated Disaster Recovery** > **ADR Bulk Adoption Configuration**.
3. On the **ADR Bulk Adoption Configuration** dialog, click **Add (+)**.
4. On the **Add ADR Bulk Adoption Configuration** dialog, in the **ADR Adopt Configuration Name** field, enter a name for the bulk configuration.
5. Select the servers you wish to add to the bulk configuration from the **Available Network Elements** panel and use the arrows to move your selection to the **Selected for bulk adoption** panel.

   You can adjust the order using the up and down arrows.

6. Click **Apply**.

### Result

The bulk configuration is created and it is now ready for use.

**Related links**

Bulk configuration utility on page 377

## Editing a bulk configuration

### About this task

Use this task to edit a bulk configuration.

### Procedure

1. Login to the Element Manager Console on the primary system or the secondary system.
2. Navigate to **Automated Disaster Recovery** > **ADR Bulk Adoption Configuration**.
3. On the **ADR Bulk Adoption Configuration** dialog, select the bulk configuration that you wish to edit and click **Edit (+-)**.
4. On the **Edit ADR Bulk Adoption Configuration** dialog, make the changes you require, using the arrow buttons.

   You cannot change the name of the bulk configuration.
5. Click **Apply**.

### Result

The bulk configuration now updated.

**Related links**

Bulk configuration utility on page 377

## Deleting a bulk configuration

### About this task

Use this task to delete a bulk configuration.

### Procedure

1. Login to the Element Manager Console on the primary system or the secondary system.
2. Navigate to **Automated Disaster Recovery** > **ADR Bulk Adoption Configuration**.
3. On the **ADR Bulk Adoption Configuration** dialog, select the bulk configuration that you wish to delete and click **Delete (-)**.

### Result

The bulk configuration is now deleted.

**Related links**

Bulk configuration utility on page 377

## Using the bulk configuration utility

### About this task

Use this task to execute a bulk configuration.

### Procedure

1. Login to the Element Manager Console on the active system.
2. Navigate to **Automated Disaster Recovery** > **ADR Bulk NEI Adoption**.
3. On the **ADR Bulk NEI Adoption** dialog, from the **Selected ADR Bulk Adoption Configuration** drop-down list, select the bulk configuration you wish to execute.
4. Click **Start**.
5. Click **Yes** on the confirmation warning dialog.

### Result

The bulk configuration begins. The Element Manager processes each network element in the order listed in the bulk configuration. It produces a report showing the status of the process. The Element Manager performs the adoption actions only on those network element instances that are not already in communication with the Element Manager. The Element Manager uses a best effort approach. If the Element Manager is unable to complete all the actions required to fully adopt a network element instance, it will continue with the next potential network element instance in the list. It the Element Manager fails over to its secondary equivalent, the bulk configuration utility does not execute on the newly active Element Manager. When the process completes, the Element Manager displays an ending message. If you re-run the same bulk configuration, the report only shows the start and end message.

**Related links**

Bulk configuration utility on page 377

# Completing the installation on both systems

### About this task

Use this task to start ADR on both systems.

### Procedure

1. Login to the Element Manager console on the primary system.
2. Navigate to **Automated Disaster Recovery** > **ADR Maintenance**.
3. Click **Start**.
4. Login to the Element Manager console on the secondary system.
5. Navigate to **Automated Disaster Recovery** > **ADR Maintenance**.
6. Click **Start**.

### Next steps

Proceed to Configuring ADR on the primary system on page 372.

# Upgrades and ADR

**Note:**

If your deployment uses virtual servers by way of VMware software, you must use the platform OVA for the secondary system. Do not use the medium simplex or medium redundant OVAs.

**Related links**

Upgrading ADR on page 381

## Upgrading ADR

If your deployment already consists of a pair of primary and secondary systems running Automatic Disaster Recovery (ADR) and you wish to upgrade them, you can stop the ADR service on both systems and upgrade the systems in the normal way using the `mcpUpgradeMR.pl` script.

### Before you begin

Stop the ADR service on both systems. You can stop the ADR service on the Element Manager Console by navigating to **Automated Disaster Recovery** > **ADR Maintenance** and clicking the **Stop** button.

### About this task

Use this task to upgrade ADR.

### Procedure

1. Log on to the primary Element Manager as a user with the AA role (for example, `ntappadm`) through `SSH` or directly at the server console.
2. At the prompt, type `cd /var/mcp/install` and press **Enter**.
3. At the prompt, type `mcpUpgradeMR.pl` and press **Enter**.

   The list of available loads is displayed.

   Avaya Aura® Conferencing loads have the filename `MCP_18.x.x.xx_2013-xx-xx-xxxx.zip`.
4. Select the load you want to upgrade to and press **Enter**.
5. Type the number of the load you want to use, and press **Enter**.

   The following message is displayed and the upgrade starts for the MCP database and Element Manager:

   ```
   --- Invoking mcpUpgrade => to upgrade the EM & Database ---
   ```

**Note:**

If the upgrade message is not displayed, stop and contact Avaya support.

Once the upgrade of the MCP database and Element Manager is complete, the following message is displayed:

```
--- EM & DataBase Upgrade Complete ---
```

6. If an error occurs (for example, due to loss of network connectivity), retry the `mcpUpgradeMR.pl` command after you resolve the problem. If an error occurs again, stop and contact Avaya support.

### Next steps

Restart the ADR service on both systems. You can start the ADR service on the Element Manager Console by navigating to **Automated Disaster Recovery** > **ADR Maintenance** and clicking the **Start** button.

#### Related links

Upgrades and ADR on page 381

## Mixing redundant primary systems and simplex secondary systems

Many customers deploy the same Avaya Aura® Conferencing model on their primary and secondary systems. For instance, if they have a large redundant primary system, they will likely have a large redundant secondary system. Similarly, if they have a medium simplex primary system, they will likely have a medium simplex secondary system, and so on.

You may wish to support Automatic Disaster Recovery (ADR) for your deployment of Avaya Aura® Conferencing using a redundant primary system and a simplex secondary system. This configuration is possible. However, Avaya does not support a configuration consisting of a simplex primary system and a redundant secondary system.

### Supported configurations

Avaya supports:

- The same model on both the primary and the secondary system for SMB, medium, and large deployments
- A large redundant primary system and a large simplex secondary system
- An SMB (or medium) redundant primary system and an SMB (or medium) simplex secondary system

### Post-installation steps

If you install a redundant model on the primary system and a simplex model on the secondary system, you must perform some post-installation steps in order for ADR to operate successfully. Specifically, you must delete any entities on the secondary system that are not part of a regular simplex model.

**Related links**

- Removing duplicate entities for a large deployment on page 383
- Removing duplicate entities for an SMB or medium deployment on page 387
- Reference configurations for SMB enterprises on page 35
- Reference configurations for medium enterprises on page 38
- Reference configurations for large enterprises on page 41
- Figuring out your ideal deployment configuration on page 48

## Removing duplicate entities for a large deployment

In these steps, the names used for the primary and secondary network elements and network element instances are the default values.

Perform these steps on the secondary system.

Ensure that you complete each of these steps in the order presented here.

### About this task

Use this task to configure a simplex secondary system for ADR in a large deployment of Avaya Aura® Conferencing.

### Procedure

1. Remove the secondary media server from the cluster configuration.
   a. On the Element Manager Console, navigate to **Feature Server Elements** > **Media Servers and Clusters** > **Media Server Clusters**.
   b. On the **Media Servers** dialog, select the second media server in the cluster (MediaServer2/MS2) and click **Delete (-)**.
   c. Click **Yes** to confirm.
2. Remove the secondary Web conferencing server from the cluster configuration.
   a. On the Element Manager Console, navigate to **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Servers and Clusters** > **Web Conferencing Server Clusters**.
   b. On the **Web Conferencing Server Clusters** dialog, select the second Web Conferencing server in the cluster (WCS2) and click **Delete (-)**.
   c. Click **Yes** to confirm.
3. Switch the collaboration library configuration write master from WCMS2 to WCMS1.
   a. On the Element Manager Console, navigate to **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Management** > **Collaboration Library**.
   b. On the **Collaboration Library** dialog, select the primary WCMS (WCMS1) from the **Write Master** drop-down list and click **Apply**.

4. Switch the Meeting Event Processor for the secondary WCMS to blank.
   a. On the Element Manager Console, navigate to **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Management** > **Web Conferencing Management Servers** > **WCMS2** > **Meeting Event Processing**.
   b. On the **WCMS2 Meeting Event Processing** dialog, select <none> from the **Meeting Event Processor** drop-down list and click **Apply**.
5. Switch the default Document Conversion Server (DCS) from the secondary DCS to the primary DCS.
   a. On the Element Manager Console, navigate to **Feature Server Elements** > **Document Conversion Servers** > **Default Document Conversion Server**.
   b. On the **Default Document Conversion Server** dialog, select the primary DCS (DCS1) from the **Document Conversion Server** drop-down list and click **Apply**.
6. Remove the secondary Web Conferencing Management Server network element instance (WCMS2_0).
   a. On the Element Manager Console, navigate to **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Management** > **Web Conferencing Management Servers** > **WCMS2_0** > **Instance**.
   b. On the **WCMS2_0 Instance** dialog, select the secondary WCMS and click **Delete (-)**.
   c. Click **Yes** to confirm.
7. Remove the secondary Web Conferencing Server network element instance (WCS2_0).
   a. On the Element Manager Console, navigate to **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Servers and Clusters** > **Web Conferencing Servers** > **WCS2_0** > **Instance**.
   b. On the **WCS2_0 Instance** dialog, select the secondary WCS and click **Delete (-)**.
   c. Click **Yes** to confirm.
8. Remove the secondary Document Conversion Server network element instance (DCS2_0).
   a. On the Element Manager Console, navigate to **Feature Server Elements** > **Document Conversion Servers** > **Document Conversion Servers** > **DCS2_0** > **Instance**.
   b. On the **DCS2_0 Instance** dialog, select the secondary DCS and click **Delete (-)**.
   c. Click **Yes** to confirm.
9. Remove the primary database (mcpdb1).
   a. On the Element Manager Console, navigate to **Feature Server Elements** > **Database** > **mcpdb** > **Configuration**.
   b. On the **mcpdb Configuration** dialog, select instance 1 for the secondary database and click **Delete (-)**.

   c. Click **Yes** to confirm.

10. Remove the secondary media server network element instance (MS2_0).

    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers** > **MS2_0** > **Instance**.

    b. On the **MS2_0 Instance** dialog, select the secondary media server and click **Delete (-)**.

    c. Click **Yes** to confirm.

11. Remove the primary application server network element instance (AS1_1).

    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Application Servers** > **AS1_1** > **Instance**.

    b. On the **AS1_1 Instance** dialog, select the secondary application server and click **Delete (-)**.

    c. Click **Yes** to confirm.

12. Remove the secondary Provisioning Manager network element instance (PROV2_0).

    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Provisioning Managers** > **PROV2_0** > **Instance**.

    b. On the **PROV2_0 Instance** dialog, select the secondary Provisioning Manager and click **Delete (-)**.

    c. Click **Yes** to confirm.

13. Remove the primary Element Manager network element instance (EM_1).

    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Element Manager** > **Element Manager** > **Instance**.

    b. On the **Element Manager Instance** dialog, select the Element Manager network element instance and click **Delete (-)**.

    c. Click **Yes** to confirm.

14. Remove the primary Accounting Manager network element instance (AM1_1).

    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Accounting Managers** > **AM1_1** > **Instance**.

    b. On the **AM1_1 Instance** dialog, select the primary Accounting Manager network element instance and click **Delete (-)**.

    c. Click **Yes** to confirm.

15. Delete the following servers:

    - MWCS2
    - EMS2

- DCS2

  a. On the Element Manager Console, navigate to **Servers**.

  b. On the **Servers** dialog, select the appropriate server from the list of servers.

  c. Click **Delete (-)**.

  d. Click **Yes** to confirm.

  e. Repeat until you have deleted the three servers.

16. Remove the secondary Web Conferencing Server network element (WCS2).

    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Server and Clusters** > **Web Conferencing Servers**.

    b. In the **Web Conferencing Servers** dialog, select WCS2 and click **Delete (-)**.

    c. Click **Yes** to confirm.

17. Remove the secondary Media Server network element (MS2).

    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers**.

    b. In the **Media Servers** dialog, select MS2 and click **Delete (-)**.

    c. Click **Yes** to confirm.

18. Remove the secondary Provisioning Manager network element (PROV2).

    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Provisioning Managers**.

    b. In the **Provisioning Managers** dialog, select PROV2 and click **Delete (-)**.

    c. Click **Yes** to confirm.

19. Delete the following logical addresses:

    - MWCSrv2MediaAddr
    - MWCSvr2IntOAMAddr
    - WCS2SvcAddr
    - EMSvr2IntOAMAddr

    a. On the Element Manager Console, navigate to **Addresses**.

    b. Select the relevant address from the **Logical Name** column and click **Delete (-)**.

    c. Click **Yes** to confirm.

    d. Repeat until you have deleted the four addresses.

### Result

You have now deleted all the duplicate entities on the secondary simplex system to ensure the effective operation of the ADR feature.

**Related links**

Mixing redundant primary systems and simplex secondary systems on page 382

## Removing duplicate entities for an SMB or medium deployment

In these steps, the names used for the primary and secondary network elements and network element instances are the default values.

Perform these steps on the secondary system.

Ensure that you complete each of these steps in the order presented here.

### About this task

Use this task to configure a simplex secondary system for ADR in an SMB or medium deployment of Avaya Aura® Conferencing.

### Procedure

1. Remove the secondary media server from the cluster configuration.
    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Media Servers and Clusters** > **Media Server Clusters**.
    b. On the **Media Servers** dialog, select the second media server in the cluster (MediaServer2/MS2) and click **Delete (-)**.
    c. Click **Yes** to confirm.
2. Remove the secondary media server network element instance (MS2_0).
    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers** > **MS2** > **Instance**.
    b. On the **MS2 Instance** dialog, select the secondary media server and click **Delete (-)**.
    c. Click **Yes** to confirm.
3. Switch the Meeting Event Processor for the secondary WCMS to blank.
    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Management** > **Web Conferencing Management Servers** > **WCMS2** > **Meeting Event Processing**.
    b. On the **WCMS2 Meeting Event Processing** dialog, select <none> from the **Meeting Event Processor** drop-down list and click **Apply**.
4. Remove the secondary Web Conferencing Management Server network element instance (WCMS2_0).
    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Management** > **Web Conferencing Management Servers** > **WCMS2_0** > **Instance**.
    b. On the **WCMS2_0 Instance** dialog, select the secondary WCMS and click **Delete (-)**.

   c. Click **Yes** to confirm.

5. Remove the secondary Document Conversion Server network element instance (DCS2_0).

   a. On the Element Manager Console, navigate to **Feature Server Elements** > **Document Conversion Servers** > **Document Conversion Servers** > **DCS2_0** > **Instance**.

   b. On the **DCS2_0 Instance** dialog, select the secondary DCS and click **Delete (-)**.

   c. Click **Yes** to confirm.

6. Remove the secondary Provisioning Manager network element instance (PROV2_0).

   a. On the Element Manager Console, navigate to **Feature Server Elements** > **Provisioning Managers** > **PROV2_0** > **Instance**.

   b. On the **PROV2_0 Instance** dialog, select the secondary Provisioning Manager and click **Delete (-)**.

   c. Click **Yes** to confirm.

7. Remove the secondary Web Conferencing Server network element instance (WCS2_0).

   a. On the Element Manager Console, navigate to **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Servers and Clusters** > **Web Conferencing Servers** > **WCS2_0** > **Instance**.

   b. On the **WCS2_0 Instance** dialog, select the secondary WCS and click **Delete (-)**.

   c. Click **Yes** to confirm.

8. Remove the primary Accounting Manager network element instance (AM1_1).

   a. On the Element Manager Console, navigate to **Feature Server Elements** > **Accounting Managers** > **AM1_1** > **Instance**.

   b. On the **AM1_1 Instance** dialog, select the primary Accounting Manager network element instance and click **Delete (-)**.

   c. Click **Yes** to confirm.

9. Remove the primary database (mcpdb1).

   a. On the Element Manager Console, navigate to **Feature Server Elements** > **Database**.

   b. On the **Database** dialog, select the primary database from the list of **Logical Database Names** and click **Delete (-)**.

   c. Click **Yes** to confirm.

10. Remove the primary application server network element instance (AS_1).

   a. On the Element Manager Console, navigate to **Feature Server Elements** > **Application Servers** > **AS_1** > **Instance**.

   b. On the **AS_1 Instance** dialog, select the secondary application server and click **Delete (-)**.

   c. Click **Yes** to confirm.

11. Remove the primary Element Manager network element instance (EM_1).

    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Element Manager** > **Element Manager** > **Instance**.

    b. On the **Element Manager Instance** dialog, select the Element Manager network element instance and click **Delete (-)**.

    c. Click **Yes** to confirm.

12. Delete the following server:

    - EMS2

    a. On the Element Manager Console, navigate to **Servers**.

    b. On the **Servers** dialog, select the appropriate server from the list of servers.

    c. Click **Delete (-)**.

    d. Click **Yes** to confirm.

13. Switch the default Document Conversion Server (DCS) from the secondary DCS to the primary DCS.

    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Document Conversion Servers** > **Default Document Conversion Server**.

    b. On the **Default Document Conversion Server** dialog, select the primary DCS (DCS1) from the **Document Conversion Server** drop-down list and click **Apply**.

14. Remove the secondary Document Conversion Server network element (DCS2).

    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Document Conversion Servers**.

    b. In the **Document Conversion Servers** dialog, select DCS2 and click **Delete (-)**.

    c. Click **Yes** to confirm.

15. Remove the secondary Web conferencing server from the cluster configuration.

    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Servers and Clusters** > **Web Conferencing Server Clusters**.

    b. On the **Web Conferencing Server Clusters** dialog, select the second Web Conferencing server in the cluster (WCS2) and click **Delete (-)**.

    c. Click **Yes** to confirm.

16. Remove the secondary Web Conferencing Server network element (WCS2).

    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Server and Clusters** > **Web Conferencing Servers**.

    b. In the **Web Conferencing Servers** dialog, select WCS2 and click **Delete (-)**.

   c. Click **Yes** to confirm.

17. Switch the collaboration library configuration write master from WCMS2 to WCMS1.

    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Management** > **Collaboration Library**.

    b. On the **Collaboration Library** dialog, select the primary WCMS (WCMS1) from the **Write Master** drop-down list and click **Apply**.

18. Remove the secondary Web Conferencing Management Server network element (WCMS2).

    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Management** > **Web Conferencing Management Servers**.

    b. In the **Web Conferencing Management Servers** dialog, select WCMS2 and click **Delete (-)**.

    c. Click **Yes** to confirm.

19. Remove the secondary Media Server network element (MS2).

    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers**.

    b. In the **Media Servers** dialog, select MS2 and click **Delete (-)**.

    c. Click **Yes** to confirm.

20. Remove the secondary Provisioning Manager network element (PROV2).

    a. On the Element Manager Console, navigate to **Feature Server Elements** > **Provisioning Managers**.

    b. In the **Provisioning Managers** dialog, select PROV2 and click **Delete (-)**.

    c. Click **Yes** to confirm.

21. Delete the following logical addresses:

    - EMSvr2IntOAMAddr
    - EMSrv2MediaAddr
    - WCS2SvcAddr

    a. On the Element Manager Console, navigate to **Addresses**.

    b. Select the relevant address from the **Logical Name** column and click **Delete (-)**.

    c. Click **Yes** to confirm.

    d. Repeat until you have deleted the three addresses.

### Result

You have now deleted all the duplicate entities on the secondary simplex system to ensure the effective operation of the ADR feature.

**Related links**

[Mixing redundant primary systems and simplex secondary systems] on page 382

# System service state

The concept of a system service state is a key concept to automatic disaster recovery (ADR). There are two system service states:

- Locked
- Unlocked

These two states equate to concepts such as online/offline, functional/not functional, or active/inactive. When Avaya Aura® Conferencing is unlocked, it is operational and providing a conferencing service. When Avaya Aura® Conferencing is locked, it is not operational and is not providing a conferencing service.

**Related links**

Changing system service state on page 391

## Changing system service state

### About this task

Use this task to change the operational status of Avaya Aura® Conferencing.

### Procedure

1. In the navigation pane of Element Manager Console, select **System Service State** > **System Service State Maintenance**.
2. Change the system service state as follows:
   - Click the **Lock** button to lock the system.
   - Click the **Unlock** button to unlock the system.

**Related links**

System service state on page 391

# Limitations of ADR

- Meeting recordings are not automatically shared between the primary and secondary Avaya Aura® Conferencing systems. Meetings recorded while the secondary system is active will not be available when the primary system is active. Meetings recorded while the primary system is active will not be available when the secondary system is active.

- The ADR functionality performs a synchronization of the data in the database between the two systems. It does not synchronize any other data/files between the two systems. This means that the data files that are stored on the WCMS in the primary system (and synchronized by way of rsync between two servers on that system) will not be available on the secondary system. In the event of a failover, you must reload all such files on to the secondary system.
- The Avaya Aura® Media Server (MS) is the only shared network element type that will automatically provide service after a switch of active systems. All other shared network element types must be adopted by the new active system in order to provide service.

# Chapter 24: Configuring a Session Border Controller (SBC)

## The session border controller acting as a router

Avaya Aura® Conferencing supports the deployment of a session border controller (SBC) between the enterprise network and the endpoints. You must deploy the SBC only at the edge of the enterprise network between the Avaya Aura® Conferencing network and Session Manager or Turnkey equivalent. In the case of a Turnkey deployment, the SBC communicates directly with the Avaya Aura® Conferencing (AAC) server. Avaya has tested and recommends the Avaya Session Border Controller for Enterprise (also known as the Sipera SBC) for use with Avaya Aura® Conferencing.

Avaya Aura® Conferencing supports the deployment of the SBC as a client application on the enterprise network. In this scenario, you do not need to administer Session Manager through System Manager, but you must add the IP address of the internal interface of SBC to the SIP firewall of Session Manager.

Avaya Aura® Conferencing supports the following different options to deploy the SBC. These deployment methods are not specific to the SBC, but are similar to administering a SIP entity. You can:

- Deploy the SBC as a client application on the enterprise network. In this scenario, you do not need to administer Session Manager through System Manager, but you must add the IP address of the internal interface of the SBC to the SIP firewall of Session Manager.
- Administer a SIP trunk between the SBC and Session Manager. In this scenario, you must administer the SIP trunk on Session Manager, and add the SBC SIP entity to the SIP firewall of Session Manager. For a Turnkey deployment, in which there is no Session Manager, Avaya Aura® Conferencing (AAC) communicates directly with the SBC by way of a SIP trunk.

### Specific configurations

If you wish to offer integrated audio and video to users, you must configure specific settings on the SBC. Similarly, if you wish to offer support for mobile devices to users, you must configure the SBC for mobile support.

For more information, see:

- Configuring external access for Avaya Aura Conferencing mobile clients on page 448
- Configuring Avaya Web Collaboration audio and video plug-in for external access on page 461

### Turnkey deployments

In an Avaya Aura® deployment, the SBC communicates with Session Manager and System Manager. In a Turnkey deployment, the SBC communicates directly with the Avaya Aura® Conferencing (AAC) server. The configuration of a Turnkey solution is largely the same as the configuration for an Avaya Aura® solution. Instead of pointing towards Session Manager and System Manager, the SBC in a Turnkey deployment points directly to the AAC and the AAC points directly to the SBC.

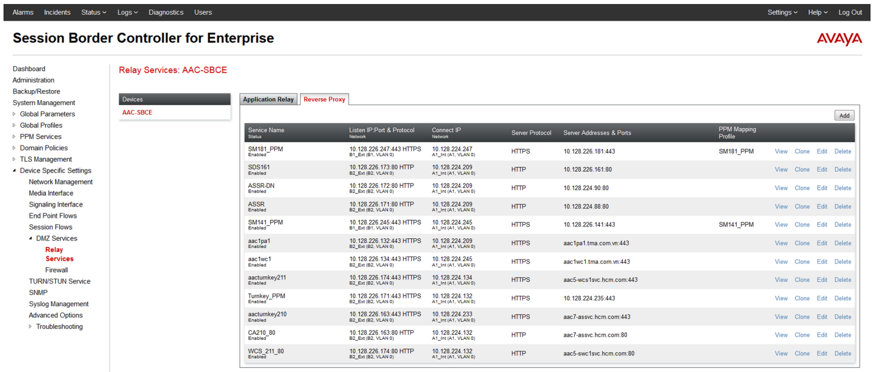
Use the links above to see the steps involved.

# The session border controller acting as a reverse proxy

Avaya Aura® Conferencing supports the deployment of a reverse proxy to provide load balancing functionality and increased security. Specifically, Avaya Aura® Conferencing supports two third-party reverse proxy servers and also offers a solution using the Avaya Session Border Controller for Enterprise as a reverse proxy server. The two third-party servers are:

- A10 Network AX Series® Application Delivery Controller
- Barracuda® Load Balancer Application Delivery Controller

Many customers prefer the option of an All-Avaya solution and for this reason, Avaya supports the deployment of the Avaya Session Border Controller for Enterprise as a reverse proxy server. When acting as a reverse proxy server, the Avaya Session Border Controller for Enterprise is limited to 300 calls (for example, 50 conferences with 6 participants in each conference with 50% screen-sharing and 50% slide-sharing). For this configuration, standard and advanced session licensing is required for each simultaneous session invoked. In addition, a mid-range server is required as a minimum, such as the Dell R210 II mid-range server.



| Service Name<br>Status | Listen IP:Port & Protocol<br>Network | Connect IP<br>Network | Server Protocol | Server Addresses & Ports | PPM Mapping Profile | |
|---|---|---|---|---|---|---|
| SM181_PPM<br>Enabled | 10.128.226.247:443 HTTPS<br>B1_Ext (B1, VLAN 0) | 10.128.224.247<br>A1_Int (A1, VLAN 0) | HTTPS | 10.128.226.181:443 | SM181_PPM | View Clone Edit Delete |
| SDS161<br>Enabled | 10.128.226.173:80 HTTP<br>B2_Ext (B2, VLAN 0) | 10.128.224.209<br>A1_Int (A1, VLAN 0) | HTTP | 10.128.226.161:80 | | View Clone Edit Delete |
| ASSR-DN<br>Enabled | 10.128.226.172:80 HTTP<br>B2_Ext (B2, VLAN 0) | 10.128.224.209<br>A1_Int (A1, VLAN 0) | HTTP | 10.128.224.90:80 | | View Clone Edit Delete |
| ASSR<br>Enabled | 10.128.226.171:80 HTTP<br>B2_Ext (B2, VLAN 0) | 10.128.224.209<br>A1_Int (A1, VLAN 0) | HTTP | 10.128.224.88:80 | | View Clone Edit Delete |
| SM141_PPM<br>Enabled | 10.128.226.245:443 HTTPS<br>B1_Ext (B1, VLAN 0) | 10.128.224.245<br>A1_Int (A1, VLAN 0) | HTTPS | 10.128.226.141:443 | SM141_PPM | View Clone Edit Delete |
| aac1pa1<br>Enabled | 10.128.226.132:443 HTTPS<br>B2_Ext (B2, VLAN 0) | 10.128.224.209<br>A1_Int (A1, VLAN 0) | HTTPS | aac1pa1.tma.com.vn:443 | | View Clone Edit Delete |
| aac1wc1<br>Enabled | 10.128.226.134:443 HTTPS<br>B2_Ext (B2, VLAN 0) | 10.128.224.245<br>A1_Int (A1, VLAN 0) | HTTPS | aac1wc1.tma.com.vn:443 | | View Clone Edit Delete |
| aacturnkey211<br>Enabled | 10.128.226.174:443 HTTPS<br>B2_Ext (B2, VLAN 0) | 10.128.224.134<br>A1_Int (A1, VLAN 0) | HTTPS | aac5-wcs1svc.hcm.com:443 | | View Clone Edit Delete |
| Turnkey_PPM<br>Enabled | 10.128.226.171:443 HTTPS<br>B2_Ext (B2, VLAN 0) | 10.128.224.132<br>A1_Int (A1, VLAN 0) | HTTPS | 10.128.224.235:443 | | View Clone Edit Delete |
| aacturnkey210<br>Enabled | 10.128.226.163:443 HTTPS<br>B2_Ext (B2, VLAN 0) | 10.128.224.233<br>A1_Int (A1, VLAN 0) | HTTPS | aac7-assvc.hcm.com:443 | | View Clone Edit Delete |
| CA210_80<br>Enabled | 10.128.226.163:80 HTTP<br>B2_Ext (B2, VLAN 0) | 10.128.224.132<br>A1_Int (A1, VLAN 0) | HTTP | aac7-assvc.hcm.com:80 | | View Clone Edit Delete |
| WCS_211_80<br>Enabled | 10.128.226.174:80 HTTP<br>B2_Ext (B2, VLAN 0) | 10.128.224.132<br>A1_Int (A1, VLAN 0) | HTTP | aac5-swc1svc.hcm.com:80 | | View Clone Edit Delete |

**Figure 22: The session border controller acting as a reverse proxy**

For more information, see Configuring Avaya Session Border Controller for Enterprise as a reverse proxy on page 427.

# Configuring a HTTP X-Forwarded-For template

## Procedure

1. Log into Avaya SBCE as root.
2. Navigate to `/usr/local/nginx/conf` and edit `proxy.conf`.
3. Uncomment the following:

   ```
   #proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
   #proxy_set_header X-Forwarded-Proto $scheme;
   ```

   **Tip:**

   Delete the # symbol to uncomment a line of code.

4. Restart the nginx services:

   ```
   /etc/init.d/nginx-data restart
   ```

# Chapter 25: Configuring an Application Delivery Controller (ADC)

## Introduction to Application Delivery Controllers (ADCs)

This section covers general requirements and a high level overview of how to deploy an Application Delivery Controller (ADC) for use with Avaya Aura® Conferencing.

Avaya recommends an ADC for providing external access as well as for providing load balancing for redundant and large deployments. The following figure shows an example deployment with redundancy.

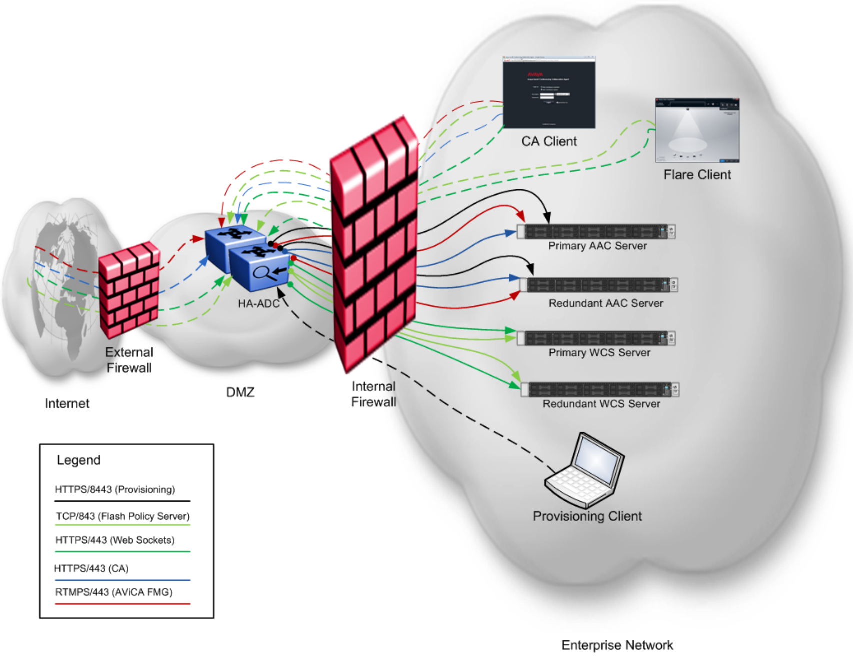


**Figure 23: External ADC Deployment**

You can deploy an additional ADC in the enterprise network if further traffic separation is required as shown in the following figure:

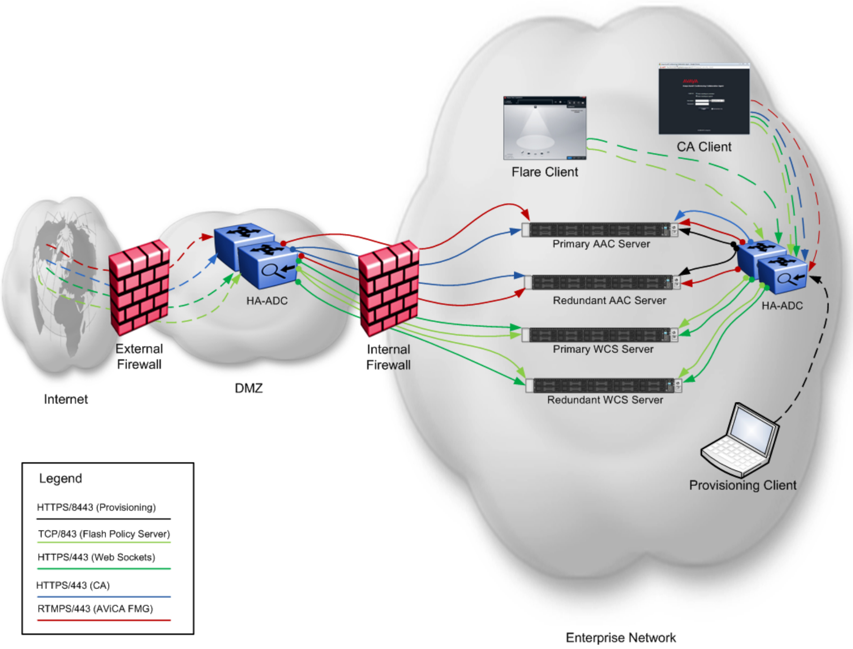


**Figure 24: Internal/External ADC Deployment**

One of the key benefits of using an ADC in the solution is that the number of firewall rules required is greatly reduced, simplifying configuration and maintenance of the solution. Additional features such as DDoS protection and Web Application Firewalls (WAF) common on ADCs can be used to enhance the defense-in-depth security of the deployment. Please refer to the specific ADC vendor documentation on how to tune these features for your deployment such that service is not impacted.

## Minimum Requirements

The follow are the minimum requirements when choosing an ADC to use with Avaya Aura® Conferencing:

- 1 Gigabit throughput
- Minimum of 10 real servers
- Layer 4 (TCP) load balancing
- Layer 7 (HTTPS) load balancing
- Web Socket support (recommended)
- HTTP Header/URL Rewriting
- Connection Persistence

## Avaya Aura® Conferencing Virtual IP Addresses

The following table lists the Virtual IP Addresses (VIP) required on the ADC for Avaya Aura® Conferencing.

**Table 24: Virtual IP Addresses (VIP)**

| Server Role | Port | VIP Type | Description |
|---|---|---|---|
| Collaboration Agent (CA) | 443 | HTTPS | A single VIP represents a pool of CA servers on the back-end. Persistence is required for connections such that once a client connects, the connection to the specific back-end server is maintained through the duration of the session. |
| Web Conferencing Server (WCS) | 443 | HTTPS \| SSL-Proxy | If the ADC supports Web Sockets, the a single HTTPS VIP represents a single WCS cluster. Note that the ADC does not do the load balancing but routes to a specific back-end WCS based on the URL. For ADC's that do not support Web Sockets, an SSL-Proxy VIP must be configured for each WCS in the cluster. |
| WCS Flash Policy Server | 843 | TCP | A single VIP represents a pool of Flash Policy Servers on the back-end. This is required for the client to retrieve the Flash policy file on initial connection. This connection does not require persistence. |
| Audio Video in Collaboration Agent | 443 \| 80 | SSL-Proxy \| HTTP | Prior to ADC support, the primary FMG for an Audio/Video in Collaboration Agent deployment did the load balancing. If this configuration is maintained, then there must be a one-to-one mapping of VIPs to back-end FMG servers. |

*Table continues…*

| Server Role | Port | VIP Type | Description |
|---|---|---|---|
| | | | Otherwise, if each back-end FMG is configured individually, then only a single VIP is required and the ADC will provide the load-balancing. If AViCA is configured to use RTMPT, the VIP type should be HTTP, or SSL-Proxy if configured for RTMPS. |
| Provisioning Manager (Prov) | 8443 | HTTPS | A single VIP representing a pool of Provisioning Manager servers on the back-end. For deployments that have an internal ADC for traffic from within the Enterprise, it is recommended to not include on the external ADC. Regardless, this interface should not be exposed to the Internet. |

# Configuring an A10 Application Delivery Controller

The A10 Network AX Series Application Delivery Controller (ADC) provides advanced load balancing as well as reverse proxy support for Web Collaboration and the Audio/Video in Collaboration Agent clients.

This configuration assumes that Avaya Aura® Conferencing is configured with transport layer security (TLS) enabled for all Web interfaces using server certificates signed by an internal Certificate Authority (CA). Typically, the internal CA is Avaya Aura® System Manager, or, as in the case of Turnkey deployments, an alternative CA. For the external side of the ADC, Avaya assumes that a third party CA, such as Verisign, is used to authenticate external clients.

You must have the following in place before you configure the ADC:

- A10 Networks AX Series appliance running ACOS version 2.7.1-P2 or above, configured with ADPs enabled for Layer 3 Virtualization (L3V).
- A10 device cabled up with network configured in routed mode for each network interface.

**Table 25: Services Required for AAC Deployment**

| Server Role | Port | VIP Type | Source NAT | Feature Templates | Notes |
|---|---|---|---|---|---|
| CA | 443 | HTTPS | Yes | • Persistence: Source-IP<br>• HTTP Template: X-Forwarded-For<br>• Health Monitor: ping<br>• Connection Reuse: TCP-reuse | |
| WCS | 443 | HTTPS* | Yes | • Persistence: Source-IP<br>• HTTP Template: X-Forwarded-For<br>• Health Monitor: ping<br>• aFleX: WCS_Clustering<br>• Connection Reuse: TCP-reuse | |
| WCS Flash Policy Server | 843 | TCP | Yes | • Persistence: Source-IP<br>• Health Monitor: ping | |
| Prov* | 8443 | HTTPS | Yes | • Persistence: Source-IP<br>• HTTP Template: X-Forwarded-For<br>• Health Monitor: ping | |

*Table continues…*

| Server Role | Port | VIP Type | Source NAT | Feature Templates | Notes |
|---|---|---|---|---|---|
| | | | | • Connection Reuse: TCP-reuse | |
| Audio/Video in Collaboration Agent (Flash Media Gateway) | 443 | SSL-Proxy | Yes | Persistence: Source-IP | |

**Related links**

Configuring the IP source NAT on page 401
Configuring IP source persistence on page 402
Configuring a HTTP X-Forwarded-For template on page 403
Installing System Manager or internal certificate authority certificates on page 404
Creating server SSL templates on page 405
Creating certificate signing requests for the virtual services on page 406
Installing signed certificates for the virtual services on page 406
Installing a certificate authority chain for the virtual services on page 407
Creating client SSL templates on page 408
Adding CA servers on page 409
Adding CA service groups on page 410
Adding a CA virtual service on page 411
Adding WCS servers on page 412
Adding WCS service groups on page 413
Configuring the WCS virtual service for WCS clusters on page 414
Adding a WCS virtual service on page 415
Adding Flash policy service groups on page 416
Adding a Flash policy server virtual service on page 417
Adding Flash Media Gateway servers on page 418
Adding Flash Media Gateway service groups on page 419
Adding a Flash Media Gateway virtual service on page 420

## Configuring the IP source NAT

You must configure the IP Source Name Address Translation (NAT) pool in order for translation from external routable addresses to internal routable addresses.

### Before you begin

Determine the pool of IPv4 addresses and netmask to use for source IP address between the A10 ADC and the Avaya Aura® Conferencing Network Elements.

### About this task

Use this task to configure the IPv4 Source NAT pool to use for the source NAT.

### Procedure

1. Log into the A10 web interface.
2. Switch to Config Mode.
3. Select **IP Source NAT** > **IPv4 Pool**.
4. Click **Add**.
5. Enter **Name**.
6. Enter **Start IP Address**.
7. Enter **End IP Address**.
8. Enter **Netmask**.
9. Click **OK**.
10. Click **Save**.

### Example

| Name | snat-pool1 |
|---|---|
| Start IP Address | 10.10.82.139 |
| End IP Address | 10.10.82.140 |
| Netmask | 255.255.255.0 |

```
ip nat pool snat-pool1 10.10.82.139 10.10.82.140 netmask /24
```

### Next steps

Proceed to Configuring IP source persistence on page 402.

#### Related links

Configuring an A10 Application Delivery Controller on page 399

## Configuring IP source persistence

Avaya Aura® Conferencing requires connections to persist for the life of each session. Once a session is established, that session is pinned to the specific internal node such that all requests for that session go to the same internal node.

### About this task

Use this task to configure the source IP Persistence policy on the A10 appliance.

### Procedure

1. Log into the A10 web interface.
2. Switch to Config Mode.

3. Select **SLB** > **Template** > **Persistent** > **Source IP Persistence**.
4. Click **Add**.
5. Enter **Name**.
6. Set **Match Type:** to **Server**.
7. Set **Timeout:** to 1200 Minutes.
8. Click **OK**.
9. Click **Save**.

### Example

```
slb template persist source-ip client-ip-persist
match-type server
timeout 1200
```

### Next steps

Proceed to Configuring HTTP X-Forwarded-For template  on page 403.

**Related links**

Configuring an A10 Application Delivery Controller on page 399

## Configuring a HTTP X-Forwarded-For template

The Avaya Aura® Conferencing Web interfaces require that the client IP address is in the HTTP headers in order to detect that a proxy is in place.

### About this task

Use this task configures the template to use in order for the client IP address to be inserted into the HTTP requests sent to the AAC from the A10 on behalf of the clients.

### Procedure

1. Log into the A10 web interface
2. Switch to **Config Mode**.
3. Select **SLB** > **Template** > **Application** > **HTTP**.
4. Click **Add**.
5. For **Name**, enter a name that represents that this template is for inserting the client IP in the headers, for example, **X-Forwarded-For**.
6. Check the check box for **Client IP Header Insert**.
7. Enter the value as **X-Forwarded-For**.
8. Click **OK**.
9. Click **Save**.

### Example

```
slb template http X-Forwarded-For
insert-client-ip X-Forwarded-For
```

### Next steps

Proceed to Installing System Manager or internal certificate authority certificate  on page 404.

#### Related links

Configuring an A10 Application Delivery Controller on page 399

## Installing System Manager or internal certificate authority certificates

By default, the Avaya Aura® Conferencing Network Elements that use TLS are using certificates signed by the System Manager Certificate Authority (CA). Therefore, in order for the A10 appliance to establish TLS connections with those Network Elements, the A10 appliance must have the System Manager CA certificate installed. If the Avaya Aura® Conferencing Network Elements are signed by some other Certificate Authority, then this procedure still applies by replacing the System Manager Certificate with the Certificate of the other Certificate Authority.

### Before you begin

You must have a PEM file for the CA certificate from the System Manager or other Certificate Authority in the case that the default System Manager Certificate Authority is not used as part of your deployment.

### About this task

Use this task to import the System Manager or other Certificate Authority certificate into the A10 appliance that is used to authentication between the A10 and the Avaya Aura® Conferencing Network Elements.

### Procedure

1. Log into the A10 web interface.
2. Switch to **Config Mode**.
3. Select **SLB** > **SSL Management** > **Certificate**..
4. Click **Import**.
5. For **Name**, enter a name that represents the CA Certificate, for example, SMGR_CA.
6. Select **Local** for **Import Certificate from**.
7. Select **PEM** for the **Certificate format**.
8. Click **Browse**, and select the PEM file of the System Manager CA certificate.
9. Click **OK**.
10. Click **Save**.

### Next steps

Proceed to Creating client SSL templates on page 408.

#### Related links

Configuring an A10 Application Delivery Controller on page 399

## Creating server SSL templates

### Before you begin

The Certificate Authority Certificates required to authenticate the internal Avaya Aura® Conferencing Network Elements are available in the A10 SSL Management. See Installing System Manager or internal certificate authority certificate on page 404.

### About this task

Use this task to create the SSL Server Templates required for the A10 to communicate with the Avaya Aura® Conferencing Network Elements. This configuration defines which Certificate Authority the A10 should use when authenticating the TLS connections to the Avaya Aura® Conferencing Network Elements.

### Procedure

1. Log into the A10 web interface.
2. Switch to **Config Mode**.
3. Select **SLB** > **Template** > **SSL** > **Server SSL**.
4. Click **Add**.
5. For **Name**, enter a name that represents this template, for example: SMGR_Server_SSL.
6. Select **TLS Version 1.0** for **TLS/SSL Version**.
7. Select **Close Notification** to enable.
8. Select the CA Certificate imported from the System Manager, for example **SMGR_CA** and click **Add**.
9. Expand the **SSL Cipher** Frame.
10. Remove all Ciphers from **Available to Servers** that do not meet your security requirements.

    At least one Cipher must be **Available to Servers**.
11. Click **OK**.
12. Click **Save**.

### Next steps

Proceed to Creating certificate signing requests for the virtual services on page 406.

#### Related links

Configuring an A10 Application Delivery Controller on page 399

## Creating certificate signing requests for the virtual services

### Before you begin

- Determine the Fully Qualified Domain Names (FQDN)s required for each of the Virtual Services to be configured on the A10.
- Decide whether to use individual certificates for each virtual service, or to use a wildcard or a SAN certificate.

### About this task

Use this task to generate Certificate Signing Requests (CSR) for each of the virtual servers to which clients connect. If you use a wildcard or SAN certificate, then you only require one CSR.

### Procedure

1. Log into the A10 web interface.
2. Switch to **Config Mode**.
3. Select **SLB** > **SSL Management** > **Certificate**.
4. Click **Create**.
5. For **File Name**, enter a name that represents this this request/certificate, for example: **VeriSignCollabAgentCert**.
6. Select **Certificate Authority** for **Issuer**.
7. Enter the FQDN for the virtual service IP in the **Common Name** field. For example: **collaborate.company.com**.
8. Select the **Country (C)** for the country.
9. Click **OK**.
10. Click **Export**, and save the CSR file.
11. Click **Cancel**.

### Next steps

Follow the specific steps from the Certificate Authority to sign the CSR. Then proceed to Installing signed certificates for the virtual services on page 406.

### Related links

Configuring an A10 Application Delivery Controller on page 399

## Installing signed certificates for the virtual services

### Before you begin

Ensure that you have the received the signed certificate back from the Certificate Authority (CA) to which you sent the Certificate Signing Request (CSR).

### About this task

Use this task to install the signed certificate associated with the CSR generated in Creating certificate signing requests for the virtual services  on page 406.

### Procedure

1. Log into the A10 web interface.
2. Switch to **Config Mode**.
3. Select **SLB** > **SSL Management** > **Certificate**.
4. Select key by name provided when the CSR was generated.
5. Select **Text** for **Import Certificate From**.
6. Select **PEM** for **Certificate Format**.
7. Cut and paste the certificate received from the Certificate Authority (CA).
8. Click **OK**.
9. Click **Save**.
10. Repeat for each signed certificate received from the CA.

### Next steps

Proceed to Installing certificate authority chain for the virtual services  on page 407.

**Related links**

Configuring an A10 Application Delivery Controller on page 399

## Installing a certificate authority chain for the virtual services

### Before you begin

Ensure that you have access to the PEM files for the root Certificate Authority as well as an intermediate Certificate Authorities used in the certificate chain.

### About this task

Use this task to install the certificate chain that is associated with the certificates identifying the virtual services. This is the certificate chain that is sent to the clients for the clients to authenticate the virtual servers.

### Procedure

1. Log into the A10 web interface.
2. Switch to **Config Mode**.
3. Select **SLB** > **SSL Management** > **Certificate**.
4. Click **Import**.
5. For **Name**, enter a name that represents the Certificate Authority chain, for example: VeriSign-CA-Chain.

6. Select  for **Import Certificate from**.
7. Select **PEM** for the **Certificate Format**.
8. Cut and paste the root certificate as well as all intermediate Certificate Authority certificates.
9. Click **OK**.
10. Click **Save**.

### Next steps

Proceed to Creating client SSL templates  on page 408.

**Related links**

Configuring an A10 Application Delivery Controller on page 399

## Creating client SSL templates

### Before you begin

Ensure that the certificate/key pair for each required certificate is in the A10 SSL Management Store. See Installing signed certificates for the virtual services  on page 406.

### About this task

Use this task to create a client SSL template for each signed certificate generated for the virtual services.

### Procedure

1. Log into the A10 web interface.
2. Switch to **Config Mode**.
3. Select **SLB** > **Template** > **SSL** > **Client SSL**.
4. Click **Add**.
5. Enter a name to represent the service client SSL, for example, **verisign_collab_ssl**.
6. Select the **Certificate Name**.
7. Select the **Chain cert name**, for example, **VeriSign-CA-Chain**.
8. Select the **Key name**, this should be the same as the **Certificate Name** above.
9. Enter the **Pass Phrase** used when creating the Certificate Signing Request (CSR).
10. Enter the **Confirm Pass Phrase**.
11. Set **SSL False Start** to **Enabled**.
12. Expand the **SSL Cipher** Frame.
13. Remove all Ciphers from **Available to Servers** that do not meet your security requirements.

At least one Cipher must be **Available to Servers**.

14. Click **OK**.
15. Click **Save**.

### Example

```
slb template client-ssl verisign_collab_ssl
cert vs-ca
chain-cert vs-chain
key vs-ca
cipher SSL3_RSA_RC4_128_SHA
```

### Next steps

Proceed to Adding CA servers  on page 409.

**Related links**

Configuring an A10 Application Delivery Controller on page 399

## Adding CA servers

### Before you begin

Determine the IPv4 addresses for each of the servers hosting the CA Network Elements that this A10 device is fronting.

### About this task

Use this task to create the server configuration for each CA Network Element. These servers make up the service group for the CA pool.

### Procedure

1. Log into the A10 web interface.
2. Switch to **Config Mode**.
3. Select **SLB** > **Service** > **Server**.
4. Click **Add**.
5. For **Name**, enter a unique name to identify the server; for example, **s_192.168.11.3**.
6. For **IP Address/Host:**, Enter the IP address; for example, **192.168.11.3**.
7. Select **ping** for **Health Monitor**.
8. Click **OK**.
9. Click **Save**.

### Example

```
slb server s_192.168.11.3 192.168.11.3
health-check ping
port 443 tcp

slb server s_192.168.11.4 192.168.11.4
```

```
health-check ping
port 443 tcp
```

### Next steps

Proceed to Adding CA service group  on page 410.

**Related links**

Configuring an A10 Application Delivery Controller on page 399

## Adding CA service groups

### Before you begin

Ensure that you have created the server configuration for each of the CA servers. See Adding CA servers  on page 409.

### About this task

Use this task to create the pool of CA servers for load balancing.

### Procedure

1. Log into the A10 web interface.
2. Switch to **Config Mode**.
3. Select **SLB** > **Service** > **Service Group**.
4. Click **Add**.
5. For **Name:**, enter a unique name to identify the service group
6. For **Type:**, select **TCP**.
7. Select **Least Connection** for the **Algorithm**.
8. Select **ping** for the **Health Monitor**.
9. For each server, in the server frame, select the server and enter **443** for the **port** and click **Add**.
10. Click **OK**.
11. Click **Save**.

### Example

```
slb service-group exampe_ca tcp
method least-connection
health-check ping
member s_192.168.11.3:443
member s_192.168.11.4:443
```

### Next steps

Proceed to Adding CA virtual service on page 411.

**Related links**

Configuring an A10 Application Delivery Controller on page 399

# Adding a CA virtual service

## Before you begin

Ensure that you have defined the following:

- Source NAT Pool
- CA Service Group
- Client SSL Template
- Server SSL Template
- Source IP Persistence Template
- X-Forwarded-For Template

## About this task

Use this task to create the virtual service for the CA. This is the interface to which users of the CA connect.

## Procedure

1. Log into the A10 web interface.
2. Switch to **Config Mode**.
3. Select **SLB** > **Service** > **Virtual Service**.
4. Click **Add**.
5. Enter the name for the CA in the **Virtual Service** field, for example, **USDC_CA**.
6. Set **Type** to **HTTPS**.
7. Set **Port** to **443**.
8. Enter the IP address for the service.

   This is the external IP address to which clients connect.
9. Select the **Service Group** for the CA.
10. Select the **Source NAT Pool**.
11. Select the **Client-SSL Template** created for the CA.
12. Select the **Server-SSL Template** created for the System Manager.
13. Select **Source IP Persistence Template** for **Persistence Template Type**.
14. Select the source IP persistence template created in Configuring IP source persistence on page 402.
15. Click **OK**.
16. Click **Save**.

## Example

```
slb virtual-server _10.10.107.226_vserver 10.10.107.226
port 443 https name USDC_CA
```

```
source-nat pool snat-pool1
service-group dev11ca1
syn-cookie
snat-on-vip
template http X-Forwarded-For
template client-ssl versign_ca
template server-ssl SMGR_Server_SSL
template persist source-ip client-ip-persist
```

#### Next steps

Proceed to Adding WCS servers on page 412.

### Related links

Configuring an A10 Application Delivery Controller on page 399

## Adding WCS servers

#### Before you begin

Ensure that you determine the IPv4 addresses for the service addresses for each of the WCS Network Elements that this A10 device is fronting.

#### About this task

Use this task to create the server configuration for each WCS Network Element. These servers make up the service group for the WCS pool.

#### Procedure

1. Log into the A10 web interface.
2. Switch to **Config Mode**.
3. Select **SLB** > **Service** > **Server**.
4. Click **Add**.
5. For **Name**, enter a unique same to identify the server, for example: **s_192.168.10.5**.
6. For **IP Address/Host**, enter the IP address of the WCS Service Address on the WCS Network Element.
7. Select **ping** for **Health Monitor**.
8. Set **Stats Data: Enabled**.
9. Set **Extended Stats: Disabled**.
10. Click **OK**.
11. Click **Save**.

#### Example

```
slb server s_192.168.10.5 192.168.10.5
health-check ping
port 443 tcp
health-check ping
```

```
slb server s_192.168.10.6 192.168.10.6
health-check ping
port 443 tcp
```

### Next steps

Proceed to Adding WCS service groups on page 413.

### Related links

Configuring an A10 Application Delivery Controller on page 399

## Adding WCS service groups

### Before you begin

Ensure that you have created the server configuration for each of the WCS servers. See Adding WCS servers on page 412.

### About this task

Use this task to create the pool of WCS servers. There should be a one-to-one mapping between the WCS Service Group and the WCS Cluster configured at the Avaya Aura® Conferencing Element Manager Console.

### Procedure

1. Log into the A10 web interface.
2. Switch to **Config Mode**.
3. Select **SLB** > **Service** > **Service Group**.
4. Click **Add**.
5. For **Name**, enter a unique name to identify the service group.
6. For **Type**, select **TCP**.
7. Select **Round Robin** for the **Algorithm**.

   **Note:**

   The Algorithm is not used for the WCS but is overridden by an aFlex script. The selection of the WCS Node is made by the Application Server and the selection at the A10 is made by a rewrite rule. Refer to the example aFlex script.
8. Select **ping** for the **Health Monitor**.
9. For each server, in the Server Frame, select the Server and enter **443** for the **Port**, and click **Add**.
10. Click **OK**.
11. Click **Save**.

### Example

```
slb service-group wcs_grp tcp
health-check ping
```

```
member s_192.168.10.53:443
member s_192.168.10.54:443
```

### Next steps

Proceed to Configuring the WCS virtual service for WCS clusters  on page 414.

### Related links

Configuring an A10 Application Delivery Controller on page 399

## Configuring the WCS virtual service for WCS clusters

### Before you begin

Ensure that you have a map of WCS short names to WCS service addresses.

### About this task

Use this task to define the aFleX script to route the WCS Cluster URI to the appropriate WCS.

### Procedure

1. Log into the A10 web interface.
2. Switch to **Config Mode**.
3. Select  **SLB** > **aFLeX**.
4. Click **Add**.
5. For **Name**, enter WCS_Clustering.
6. For **Definition**, enter the aFleX script to remove the WCS short name from the URI and send to the appropriate WCS service address.

   An example is provided below.
7. Click **OK**.
8. Click **Save**.

### Example

```
when HTTP_REQUEST {
set WCS1_SHORT_NAME "WCS1"
set WCS1_NODE 192.168.10.5
set WCS2_SHORT_NAME "WCS2"
set WCS2_NODE 192.168.10.6

if { ([HTTP::uri] contains $WCS1_SHORT_NAME) } {
    regsub "$WCS1_SHORT_NAME/" [HTTP::uri] {} newURI
    HTTP::uri $newURI
    node $WCS1_NODE

} elseif { ([HTTP::uri] contains $WCS2_SHORT_NAME) } {
    regsub "$WCS2_SHORT_NAME/" [HTTP::uri] {} newURI
    HTTP::uri $newURI
    node $WCS2_NODE     } }
```

### Next steps

Proceed to Adding a WCS virtual service on page 415.

**Related links**

Configuring an A10 Application Delivery Controller on page 399

## Adding a WCS virtual service

### Before you begin

Ensure that you have defined the following:

- Source NAT Pool
- WCS Service Group
- Client SSL Template
- Server SSL Template
- Source IP Persistence Template
- aFlex WCS Cluster Script

### About this task

Use this task to create the virtual service for the WCS. This is the interface to which users of the WCS Cluster connect.

### Procedure

1. Log into the A10 web interface.
2. Switch to **Config Mode**.
3. Select **SLB** > **Service** > **Virtual Service**.
4. Click **Add**.
5. Enter the name for the WCS in the **Virtual Service** field, for example, **USDC_WCS**.
6. Set **Type** to **HTTPS**.
7. Set **Port** to **443**.
8. Enter the IP address for the service.
9. Select the **Service Group** for the WCS.
10. Select the **Source NAT Pool**.
11. Select the **Client-SSL Template** created for the WCS.
12. Select the **Server-SSL Template** created for the System Manager.
13. Select **Source IP Persistence Template** for **Persistence Template Type**.
14. Select the source IP persistence template created in Configuring IP source persistence on page 402.

15. Click **OK**.
16. Click **Save**.

### Example

```
slb virtual-server _10.10.107.227_vserver 10.10.107.227

port 843 tcp
    name USDC_FP
    source-nat pool snat-pool1
    service-group fp_grp
    syn-cookie
    snat-on-vip
    template persist source-ip client-ip-persist

port 443 https
    name USDC_WCS
    source-nat pool snat-pool1
    service-group wcs_grp
    syn-cookie
    snat-on-vip
    template http X-Forwarded-For
    template client-ssl verisign-wcs
    template server-ssl AvayaITCA
    template connection-reuse tcp-reuse
    template persist source-ip client-ip-persist
    aflex WCS_Clustering
```

### Next steps

Proceed to Add Flash policy server service groups  on page 416.

**Related links**

Configuring an A10 Application Delivery Controller on page 399

## Adding Flash policy service groups

### Before you begin

The Flash Policy Server is co-resident with the WCS Server therefore it shares the same server configuration on the A10. See Adding WCS servers on page 412 to configure the appropriate server configuration prior to beginning this task.

### About this task

Use this task to create the pool of Flash Policy servers. There should be a one-to-one mapping between the Flash Policy Service Group and the WCS Cluster configured at the Avaya Aura® Conferencing Element Manager Console.

### Procedure

1. Log into the A10 web interface.
2. Switch to **Config Mode**.
3. Select **SLB** > **Service** > **Service Group**.
4. Click **Add**.

5. For **Name**, enter a unique name to identify the service group.
6. For **Type**, select **TCP**.
7. Select **Least Connection** for the **Algorithm**.
8. Select **ping** for the **Health Monitor**.
9. For each server, in the Server Frame, select the Server and enter **843** for the **Port**, and click **Add**.

   **Note:**

   The server is the same server used for the WCS.
10. Click **OK**.
11. Click **Save**.

### Example

```
slb service-group fp-grp tcp
method least-connection
health-check ping
member s_192.168.10.53:843
member s_192.168.10.54:843
```

### Next steps

Proceed to Adding a Flash policy server virtual service on page 417.

**Related links**

Configuring an A10 Application Delivery Controller on page 399

## Adding a Flash policy server virtual service

### Before you begin

Ensure that you have defined the following:

- Source NAT Pool
- Flash Policy Service Group

### About this task

Use this task to create the virtual service for the Flash Policy Server.

### Procedure

1. Log into the A10 web interface.
2. Switch to **Config Mode**.
3. Select **SLB** > **Service** > **Virtual Service**.
4. Click **Add**.
5. Enter the name for the Flash Policy Server Virtual Service in the **Virtual Service** field, for example, **USDC_FPS**.

6. Set **Type** to **TCP-Proxy**.
7. Set **Port** to **843**.
8. Enter the IP address for the service.
9. Select the **Service Group** for the Flash Policy Server.
10. Select the **Source NAT Pool**.
11. Click **OK**.
12. Click **Save**.

### Example

```
slb virtual-server _10.10.107.227_vserver 10.10.107.227
port 843  tcp
    name USDC_FPS
    source-nat pool snat-pool1
    service-group dev11fp
    syn-cookie
    snat-on-vip
    temp    late persist source-ip client-ip-persist
```

### Related links

Configuring an A10 Application Delivery Controller on page 399

## Adding Flash Media Gateway servers

### Procedure

1. Log into the A10 web interface.
2. Switch to **Config Mode**.
3. Select **SLB** > **Service** > **Server**.
4. Click **Add**.
5. For **Name**, enter a unique same to identify the FMG server, for example: **s_192.168.10.55**.
6. For **IP Address/Host**, enter the IP address, for example: **s_192.168.10.55**.
7. Select **ping** for **Health Monitor**.
8. Click **OK**.
9. Click **Save**.
10. Repeat these steps to create the configuration for each server running a FMG.

### Example

```
slb server s_192.168.10.55 192.168.10.55
    health-check ping
    port 443  tcp
        health-check ping

slb server s_192.168.10.56 192.168.10.56
    health-check ping
    port 443  tcp
        health-check ping
```

### Next steps

Proceed to Adding Flash Media Gateway service groups on page 419.

### Related links

Configuring an A10 Application Delivery Controller on page 399

## Adding Flash Media Gateway service groups

### Before you begin

Ensure that you have configured each of the Flash Media Gateway (FMG) servers. See Adding Flash Media Gateway servers on page 418.

### About this task

Use this task to create the pool of Flash Media Gateway servers.

### Procedure

1. Log into the A10 web interface.
2. Switch to **Config Mode**.
3. Select **SLB** > **Service** > **Service Group**.
4. Click **Add**.
5. For **Name**, enter a unique name to identify the service group.
6. For **Type**, select **TCP**.
7. Select **Least Connection** for the **Algorithm**.
8. Select **ping** for the **Health Monitor**.
9. For each server, in the Server Frame, select the Server and enter **443** for the **Port**, and click **Add**.
10. Click **OK**.
11. Click **Save**.

### Example

```
slb service-group fmg_grp tcp
    method least-connection
    health-check ping
    reset-on-server-selection-fail
    member s_192.168.10.55:443
    member s_135.168.10.56:443
```

### Next steps

Proceed to Adding a Flash Media Gateway virtual service on page 420.

**Related links**

Configuring an A10 Application Delivery Controller on page 399

## Adding a Flash Media Gateway virtual service

### Before you begin

Ensure that you have defined the following:

- Source NAT Pool
- Flash Policy Service Group
- Client SSL Template
- Server SSL Template
- Source IP Persistence Template

### About this task

Use this task to create the virtual service for the Flash Media Gateway (FMG).

### Procedure

1. Log into the A10 web interface.
2. Switch to **Config Mode**.
3. Select **SLB** > **Service** > **Virtual Service**.
4. Click **Add**.
5. Enter the name for the FMG in the **Virtual Service** field, for example, **USDC_FMG**.
6. Set **Type** to **SSL-Proxy**.
7. Set **Port** to **443**.
8. Enter the IP address for the service.
9. Select the **Service Group** for the FMG.
10. Enable **Source NAT traffic against VIP**
11. Select the **Source NAT Pool**.
12. Select the **Client-SSL Template** created for the FMG.
13. Select the **Source IP Persistence Template** for the **Persistence Template Type**.
14. Click **OK**.
15. Click **Save**.

### Example

```
slb virtual-server _10.10.107.228_vserver 10.10.107.228
port 443  ssl-proxy
name USDC_FMG
source-nat pool snat-pool1
service-group fmg-grp
```

```
template client-ssl verisign-fmg
template server-ssl SMGR_CA
template persist source-ip client-ip-persist
```

**Related links**

Configuring an A10 Application Delivery Controller on page 399

# Configuring a Barracuda load balancer application delivery controller

The Barracuda Load Balancer Application Delivery Controller (ADC) provides advanced load balancing and reverse proxy support for Web Collaboration as well as for the Audio/Video in Collaboration Agent clients.

This configuration assumes that Avaya Aura® Conferencing is configured with TLS enabled for all web interfaces using server certificates signed by an internal certificate authority (CA). Normally, the internal certificate authority (CA) is the certificate authority component of the Avaya Aura® System Manager. For the external side of the ADC, it is assumed that a third party certificate authority, for example, Verisign, is used so that external clients can authenticate the servers.

**Note:**

The Barracuda ADC does not provide a means to import enterprise Certificate Authorities (CA) into its trust store. Therefore, unless the Avaya Aura® Conferencing network elements are using certificates signed by a well-known public certificate authority, then certificate validation between the ADC and the Avaya Aura® Conferencing network elements must be disabled otherwise validation fails.

You must have the following in place before you configure the ADC:

- Barracuda Load Balancer ADC running 3.6.1.011 or greater
- The Barracuda Load Balancer cabled and configured in **Route-Path** mode

**Table 26: Services Required for AAC Deployment**

| Server Role | Port | VIP Type | Source NAT | Feature Templates | Notes |
|---|---|---|---|---|---|
| CA | 443 | HTTPS | Yes | • Persistence: Source-IP<br>• Health Monitor: TCP Port Check<br>• Connection Pooling | |

*Table continues…*

| Server Role | Port | VIP Type | Source NAT | Feature Templates | Notes |
|---|---|---|---|---|---|
| WCS | 443 | Secure TCP Proxy | Yes | • Persistence: Source-IP<br>• Health Monitor: TCP Port Check | |
| WCS Flash Policy Server | 843 | TCP Proxy | Yes | • Persistence: Source-IP<br>• Health Monitor: TCP Port Check | |
| Prov | 8443 | HTTPS | Yes | • Persistence: Source-IP<br>• Health Monitor: TCP Port Check | |
| Audio/Video in Collaboration Agent (Flash Media Gateway) | 443 | Secure TCP Proxy | Yes | • Persistence: Source-IP<br>• Health Monitor: TCP Port Check | |

**Related links**

Creating certificates on page 422
Adding a CA service on page 423
Adding a WCS service on page 424
Adding a Flash policy service on page 425
Adding a Flash media gateway service on page 426

# Creating certificates

## Before you begin

- Determine the fully qualified domain names (FQDN)'s required for each of the Virtual Services to be configured on the Barracuda ADC.
- Decide whether to use individual certificates for each virtual service, or to use a wildcard or a SAN certificate.

## About this task

Use these steps to upload certificates for each of your virtual servers that clients will connect to. If a wildcard or SAN certificate is used, then only one is required.

### Procedure

1. Log into the Barracuda web interface.
2. Navigate to **Basic** > **Certifcates**.
3. Upload the required certificates.

### Next steps

Proceed to Adding a CA service on page 423.

**Related links**

Configuring a Barracuda load balancer application delivery controller on page 421

## Adding a CA service

### Before you begin

- Determine the IPv4 addresses for each of the servers hosting the CA network elements that this Barracuda device is fronting.
- Update the Domain Name Server (DNS) for the CA Service FQDN.
- Load the certificate for the CA Service FQDN on the Barracuda device.

### About this task

Use these steps to create the virtual service for the CA. This is the interface to which users of the CA connect.

### Procedure

1. Log into the Barracuda web interface.
2. Navigate to **Basic** > **Services**.
3. Expand **Add New Service**.
4. For **Service Name**, enter a unique name to identify this service, for example, **USDC_CA**.
5. Select **Layer 7 - HTTPS** for **Service Type**.
6. Enter the **Virtual IP Address** that is associated with the CA Service FQDN.
7. Leave the **Port** set to **443**.
8. Select the **SSL Certificate** defined for this service.
9. Select **WAN** for **Interface**.
10. Add a **Real Server** for each CA instance that is associated with this Service FQDN.
11. Click **Add Service**.
12. Edit the advanced Real Server settings by clicking the **Edit** graphic next to the Real Server.
13. Under SSL, set **Enable HTTPS/SSL** to **Yes** and **Validate Certificate** to **No.**

These settings are required in order for the internal link between the Barracuda and the Avaya Aura® Conferencing servers to use TLS. If you want to set Validate Certificate to Yes, the Avaya Aura® Conferencing servers must use publicly signed certificates internally.

14. Click **Save Changes**.
15. Repeat steps 12-14 for each Real Server defined for this service.
16. Edit the advanced service settings by clicking the **Edit** graphic next to the service.
17. Under **Persistence**, set **PersistenceType** to **Client IP**.
18. Click **Save Changes**.

### Next steps

Proceed to Adding a WCS service on page 424.

**Related links**

Configuring a Barracuda load balancer application delivery controller on page 421

## Adding a WCS service

### Before you begin

- Determine the IPv4 addresses for each of the servers hosting the WCS network elements that this Barracuda device is fronting.
- Update the Domain Name Server (DNS) for the WCS Service FQDN.
- Load the certificate for the WCS Service FQDN on the Barracuda device.

**Note:**

Barracuda does not support Web Sockets, therefore, the Avaya Aura® Conferencing WCS Cluster FQDN is not used and each WCS must have an external routable FQDN that is reachable by the clients.

### About this task

Use these steps to create the virtual service for the CA. This is the interface to which users of the CA connect.

### Procedure

1. Log into the Barracuda web interface.
2. Navigate to **Basic** > **Services**.
3. Expand **Add New Service**.
4. For **Service Name**, enter a unique name to identify this service, for example, **USDC_WCS1**.
5. Select **Secure TCP Proxy** for **Service Type**.
6. Enter the **Virtual IP Address** that is associated with the WCS Service FQDN.

7. Leave the **Port** set to **443**.
8. Select the **SSL Certificate** defined for this service.
9. Select **WAN** for **Interface**.
10. Add a **Real Server** for the WCS that is associated with this Service FQDN.
11. Click **Add Service**.
12. Edit the advanced Real Server settings by clicking the **Edit** graphic next to the Real Server.
13. Under SSL, set **Enable HTTPS/SSL** to **Yes** and **Validate Certificate** to **No.**

    These settings are required in order for the internal link between the Barracuda and the Avaya Aura® Conferencing servers to use TLS. If you want to set Validate Certificate to Yes, the Avaya Aura® Conferencing servers must use publicly signed certificates internally.
14. Click **Save Changes**.
15. Edit the advanced service settings by clicking the **Edit** graphic next to the service.
16. Under **Persistence**, set **PersistenceType** to **Client IP**.
17. Click **Save Changes**.

### Next steps

Proceed to Adding a Flash policy service on page 425.

#### Related links

Configuring a Barracuda load balancer application delivery controller on page 421

## Adding a Flash policy service

### Before you begin

- Determine the WCS service.
- Determine the IPv4 addresses for each of the servers hosting the WCS network elements that this Barracuda device is fronting.
- Update the Domain Name Server (DNS) for the WCS Service FQDN.

### About this task

Use these steps to create the virtual service for each Flash Policy Service that is associated with each WCS.

### Procedure

1. Log into the Barracuda web interface.
2. Navigate to **Basic** > **Services**.
3. Expand **Add New Service**.

4. For **Service Name**, enter a unique name to identify this service, for example, **USDC _FPS1**.
5. Select **TCP Proxy** for **Service Type**.
6. Enter the **Virtual IP Address** that is associated with the WCS Service FQDN.
7. Leave the **Port** set to **843**.
8. Select **WAN** for **Interface**.
9. Add a **Real Server** for the WCS that is associated with this Service FQDN.
10. Click **Add Service**.

### Next steps

Proceed to Adding a Flash media gateway service  on page 426.

**Related links**

Configuring a Barracuda load balancer application delivery controller on page 421

## Adding a Flash media gateway service

### Before you begin

- Determine the Flash Media Gateway (FMG) Service IPv4 addresses for each of the servers hosting an FMG that this Barracuda device is fronting.
- Update the Domain Name Server (DNS) for each FMG Service FQDN.
- If you are using Real Time Messaging Protocol with SSL (RTMPS), load a certificate for each FMG Service FQDN on the Barracuda device.

**Note:**

If the FMGs are not grouped into a cluster which is managed by a primary FMG, you can configure them such that there is only one FMG Service address on the Barracuda with a pool of Real Servers for each individual FMG. In this way, the Barracuda can balance the load but also reduce the number of public-facing IP addresses and certificates.

### About this task

Use this steps to create the virtual service for each FMG that is used by Audio/Video in Collaboration Agent.

### Procedure

1. Log into the Barracuda web interface.
2. Navigate to **Basic** > **Services**.
3. Expand **Add New Service**.
4. For **Service Name**, enter a unique name to identify this service, for example, **USDC_FMGS1**.
5. Configure the **Service Type** as follows:

| Choice Option | Choice Description |
|---|---|
| **If you are using RTPMT** | Select **Layer 7 - HTTP** for the **Service Type**. |
| **If you are using RTPMS** | Select **Secure TCP Proxy** for the **Service Type**. |

6. Enter the **Virtual IP Address** that is associated with the WCS Service FQDN.
7. Configure the **Port** as follows:

| Choice Option | Choice Description |
|---|---|
| **If you are using RTPMT** | Set the **Port** to **80**. |
| **If you are using RTPMS** | Leave the **Port** set to **443**. |

8. If using RTMPS, select the **SSL Certificate** defined for this service.
9. Select **WAN** for **Interface**.
10. Add a **Real Server** for the FMG instance that is associated with this Service FQDN.
11. Click **Add Service**.
12. Edit the advanced Real Server settings by clicking the **Edit** graphic next to the Real Server.
13. Under SSL, set **Enable HTTPS/SSL** to **Yes** and **Validate Certificate** to **No.**

    These settings are required in order for the internal link between the Barracuda and the Avaya Aura® Conferencing servers to use TLS. If you want to set Validate Certificate to Yes, the Avaya Aura® Conferencing servers must use publicly signed certificates internally.
14. Click **Save Changes**.
15. Edit the advanced service settings by clicking the **Edit** graphic next to the service.
16. Under **Persistence**, set **PersistenceType** to **Client IP**.
17. Click **Save Changes**.

**Related links**

Configuring a Barracuda load balancer application delivery controller on page 421

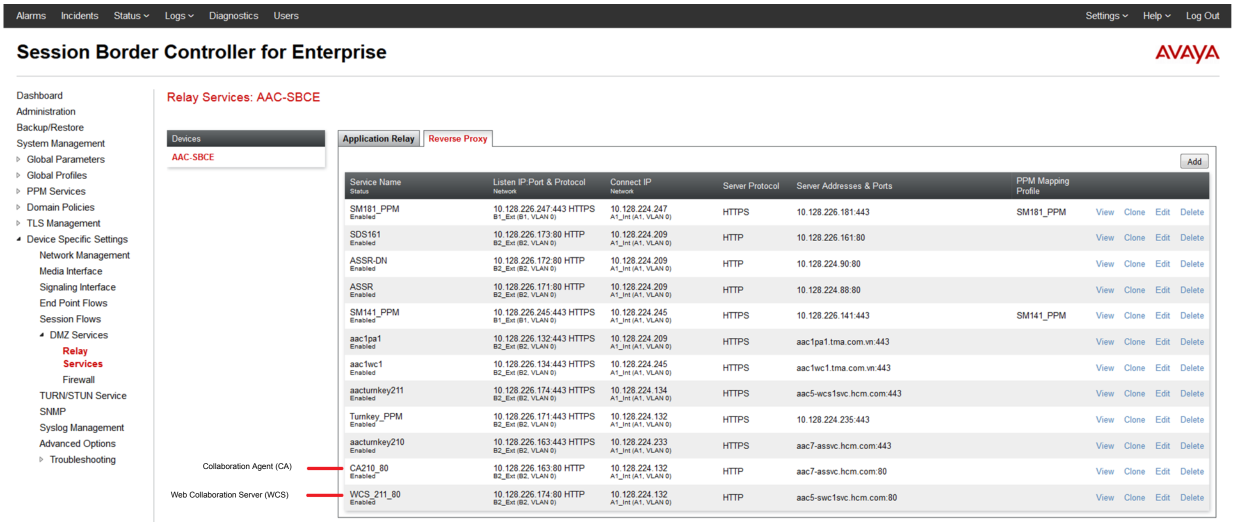
# Configuring Avaya Session Border Controller for Enterprise as a reverse proxy

This section describes how to configure Avaya Session Border Controller for Enterprise to act as a reverse proxy to enable remote workers to access the complete Avaya Aura® Conferencing solution from the public internet, including the Collaboration Agent, data sharing aspects of conferences, and the Flash-based method[9] of integrated audio and video. In order to offer the

[9] For more information on the non-Flash method of integrated audio and video, see Deploying integrated audio and video on page 518.

Collaboration Agent, data sharing aspects of a conference, and the Flash-based method of integrated audio and video, you must enable secure access from the public internet to three servers:

- Collaboration Agent server
- Web Collaboration server (WCS)
- Flash Media Gateway (FMG) server



Relay Services: AAC-SBCE

| Service Name<br>Status | Listen IP:Port & Protocol<br>Network | Connect IP<br>Network | Server Protocol | Server Addresses & Ports | PPM Mapping Profile | | | | |
|---|---|---|---|---|---|---|---|---|---|
| SM181_PPM<br>Enabled | 10.128.226.247:443 HTTPS<br>B1_Ext (B1, VLAN 0) | 10.128.224.247<br>A1_Int (A1, VLAN 0) | HTTPS | 10.128.226.181:443 | SM181_PPM | View | Clone | Edit | Delete |
| SDS161<br>Enabled | 10.128.226.173:80 HTTP<br>B2_Ext (B2, VLAN 0) | 10.128.224.209<br>A1_Int (A1, VLAN 0) | HTTP | 10.128.226.161:80 | | View | Clone | Edit | Delete |
| ASSR-DN<br>Enabled | 10.128.226.172:80 HTTP<br>B2_Ext (B2, VLAN 0) | 10.128.224.209<br>A1_Int (A1, VLAN 0) | HTTP | 10.128.224.90:80 | | View | Clone | Edit | Delete |
| ASSR<br>Enabled | 10.128.226.171:80 HTTP<br>B2_Ext (B2, VLAN 0) | 10.128.224.209<br>A1_Int (A1, VLAN 0) | HTTP | 10.128.224.88:80 | | View | Clone | Edit | Delete |
| SM141_PPM<br>Enabled | 10.128.226.245:443 HTTPS<br>B1_Ext (B1, VLAN 0) | 10.128.224.245<br>A1_Int (A1, VLAN 0) | HTTPS | 10.128.226.141:443 | SM141_PPM | View | Clone | Edit | Delete |
| aac1pa1<br>Enabled | 10.128.226.132:443 HTTPS<br>B2_Ext (B2, VLAN 0) | 10.128.224.209<br>A1_Int (A1, VLAN 0) | HTTPS | aac1pa1.tma.com.vn:443 | | View | Clone | Edit | Delete |
| aac1wc1<br>Enabled | 10.128.226.134:443 HTTPS<br>B2_Ext (B2, VLAN 0) | 10.128.224.245<br>A1_Int (A1, VLAN 0) | HTTPS | aac1wc1.tma.com.vn:443 | | View | Clone | Edit | Delete |
| aacturnkey211<br>Enabled | 10.128.226.174:443 HTTPS<br>B2_Ext (B2, VLAN 0) | 10.128.224.134<br>A1_Int (A1, VLAN 0) | HTTPS | aac5-wcs1svc.hcm.com:443 | | View | Clone | Edit | Delete |
| Turnkey_PPM<br>Enabled | 10.128.226.171:443 HTTPS<br>B2_Ext (B2, VLAN 0) | 10.128.224.132<br>A1_Int (A1, VLAN 0) | HTTPS | 10.128.224.235:443 | | View | Clone | Edit | Delete |
| aacturnkey210<br>Enabled | 10.128.226.163:443 HTTPS<br>B2_Ext (B2, VLAN 0) | 10.128.224.233<br>A1_Int (A1, VLAN 0) | HTTPS | aac7-assvc.hcm.com:443 | | View | Clone | Edit | Delete |
| CA210_80<br>Enabled | 10.128.226.163:80 HTTP<br>B2_Ext (B2, VLAN 0) | 10.128.224.132<br>A1_Int (A1, VLAN 0) | HTTP | aac7-assvc.hcm.com:80 | | View | Clone | Edit | Delete |
| WCS_211_80<br>Enabled | 10.128.226.174:80 HTTP<br>B2_Ext (B2, VLAN 0) | 10.128.224.132<br>A1_Int (A1, VLAN 0) | HTTP | aac5-swc1svc.hcm.com:80 | | View | Clone | Edit | Delete |

**Figure 25: Collaboration Agent and WCS on the Avaya Session Border Controller for Enterprise interface**

For this configuration to operate successfully, you require at least one external IP address for the Collaboration Agent server, at least one external IP address for the Web Collaboration server (WCS), and at least one external IP address for the Flash Media Gateway (FMG) server. You also require one internal IP address for the Collaboration Agent, WCS, and FMG servers. Each interface should contain IPs from the same subnet. Avaya recommends that the internal IP address of the Avaya SBCE should be in the same subnet as the service IP address of the Collaboration Agent, the WCS Server, and the FMG server.

You require security certificates for this configuration. You can use certificates that are signed by System Manager. Alternatively, you can use certificates that are signed by a Certificate Authority other than the System Manager. The procedures in this section use certificates that are signed by System Manager.

These steps require a technical knowledge of the Avaya Session Border Controller for Enterprise. The Avaya Session Border Controller for Enterprise is often referred to as Avaya SBCE.

To avoid confusion, this section adheres to the following naming conventions:

- CA refers to Certificate Authority
- Collaboration Agent refers to the Collaboration Agent server
- WCS refers to Web Collaboration Server

- FMG refers to Flash Media Gateway

**Related links**

Checklist for configuring Avaya Aura Conferencing and the Avaya SBCE on page 429
Configuring your network for the proxy service on page 432
Retrieving Collaboration Agent, FMG, and WCS certificates and key files from the Avaya Aura Conferencing system on page 433
Retrieving the System Manager CA certificate on page 435
Installing the System Manager CA certificate on page 435
Installing the Collaboration Agent, WCS, and FMG certificates on page 436
Creating client profiles for the Collaboration Agent, WCS, and FMG on page 438
Creating server profiles for the Collaboration Agent, WCS, and FMG on page 441
Creating a reverse proxy for the Collaboration Agent, WCS, and FMG on page 444
Configuring the Flash policy for the WCS on page 446

## Checklist for configuring Avaya Aura® Conferencing and the Avaya SBCE

The following table provides a high-level view of the tasks involved in configuring Avaya Aura® Conferencing and the Avaya SBCE.

**Tip:**

Print this checklist so that you can mark each task as you complete it.

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Add the following IP addresses:<br>• At least one external IP for Collaboration Agent<br>• At least one external IP for WCS<br>• At least one external IP for FMG<br>• At least one internal IP for Collaboration Agent, WCS, and FMG | Configuring your network for the proxy service on page 432 | Make a note of these external and internal IPs. You require them for several tasks, such as Configuring the reverse proxy on page 444 and Configuring the Flash policy for the WCS on page 446. | |

*Table continues…*

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 2 | Ensure that you have created a System Manager- signed certificate or a third party authority-signed certificate, such as Verisign for each network element: Collaboration Agent, WCS, and FMG. | Creating identity certificates signed by System Manager on page 564 | If you are using RTMPS for the Flash clients, this step is necessary. | |
| 3 | Obtain the Collaboration Agent, FMG, and WCS certificates from Avaya Aura® Conferencing | Retrieving Collaboration Agent, FMG, and WCS certificates and key files from the Avaya Aura Conferencing system on page 433 | | |
| 4 | For the FMG server only: Perform some additional security-related steps | • Creating a System Manager- signed certificate for the Flash Media Gateway IP address on page 543<br>• Creating a VeriSign-signed certificate for the Flash Media Gateway on page 543<br>• Securing the JMX connection between the Flash Media Gateways and the RTMPS connection to the Flash Media Gateway Management server on page 545<br>• Configuring a secure SIP TLS connection from the Flash Media Gateway to Avaya Aura Session Manager on page 546<br>• Configuring a secure RTMPS connection between the Flash Media Gateways and the Audio/ Video in Collaboration | These tasks are from the Deploying integrated audio and video chapter. Ensure that you return to the current checklist to complete the steps to configure the reverse proxy. | |

*Table continues…*

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| | | Agent clients on page 547 | | |
| 5 | Obtain the root certificate authority from System Manager | Retrieving the System Manager CA certificate on page 435 | This procedure uses certificates signed by System Manager. As an alternative, you can use third party certificates. For more information on third party certificates, see Introduction to certificates on page 552. | |
| 6 | Add the root certificate authority from System Manager to the Avaya SBCE | Installing the System Manager CA certificate on page 435 | | |
| 7 | Add the Collaboration Agent, WCS, and FMG certificates to the Avaya SBCE | Installing the Collaboration Agent, WCS, and FMG certificates on page 436 | You must perform this task for each server: Collaboration Agent, WCS and FMG. | |
| 8 | Create client profiles for the Collaboration Agent, WCS, and FMG | Creating client profiles for the Collaboration Agent, WCS, and FMG on page 438 | You must perform this task for each server: Collaboration Agent, WCS and FMG. | |
| 9 | Create server profiles for the Collaboration Agent, WCS, and FMG | Creating server profiles for the Collaboration Agent, WCS, and FMG on page 441 | You must perform this task for each server: Collaboration Agent, WCS and FMG. | |
| 10 | Configure the reverse proxy service | Configuring the reverse proxy on page 444 | You must perform this task for each server: Collaboration Agent, WCS and FMG. | |
| 11 | Configure the Flash policy for WCS | Configuring the Flash policy for the WCS on page 446 | Perform this step only if you are configuring the WCS. This step is not needed for the FMG or Collaboration Agent. | |

**Related links**

Configuring Avaya Session Border Controller for Enterprise as a reverse proxy on page 427

## Configuring your network for the proxy service

With the Network Management function of the Device Specific Settings feature, you can configure the network and network interface settings affecting the Avaya SBCE security devices deployed throughout the enterprise. You can configure many networks, network interfaces, and Virtual LANs (VLANs).

When you install an Avaya SBCE security device, certain network-specific information is defined, such as device IP addresses, public IP addresses, netmask, and gateway to interface the device to the network. For information about installing a Avaya SBCE device, see *Installing an Avaya SBCE device*. The network-specific information populates various **Network Management** tabs. To optimize the device performance and network efficiency, you can change the information.

You require at least one external IP address for the Collaboration Agent server, one external IP address for the Web Collaboration Server (WCS), and one external IP address for the Flash Media Gateway (FMG) server. You also require at least one internal IP address to connect to the Collaboration Agent, WCS servers, and FMG servers. Each interface should contain IPs from the same subnet. Avaya recommends that the internal IP address of the Avaya SBCE should be in the same subnet as the service IP address of the Collaboration Agent, the WCS Server, and the FMG server.

### About this task

Use this task to configure your network for the proxy service.

### Before you begin

Log into Avaya SBCE.

### Procedure

1. Log on to the EMS web interface using the administrator credentials.
2. In the left navigation pane, click **Device Specific Settings** > **Network Management**.

   The system displays the Network Management page.
3. On the **Networks** tab, in the Devices section, click the Avaya SBCE security device of which you want to edit the parameters.
4. Click **Edit** corresponding to network that you want to edit.

   If the network does not exist, click **Add** to add a new network.

   The system displays the Add Network or Edit Network page.
5. Edit the network field descriptions and click **Finish**.

### Related links

Configuring Avaya Session Border Controller for Enterprise as a reverse proxy on page 427
Edit network field descriptions on page 433

## Edit network field descriptions

You require at least one external IP address for the Collaboration Agent server, one external IP address for the Web Collaboration Server (WCS), and one external IP address for the Flash Media Gateway (FMG) server. You also require at least one internal IP address to connect to the Collaboration Agent, WCS servers, and FMG servers. Each interface should contain IPs from the same subnet. Avaya recommends that the internal IP address of the Avaya SBCE should be in the same subnet as the service IP address of the Collaboration Agent, the WCS Server, and the FMG server.

| Name | Description |
|---|---|
| **Name** | Specifies the network name. |
| **Default Gateway** | Specifies the default gateway of the network. |
| **Subnet Mask** | Specifies the subnet mask of the network. |
| **Interface** | Specifies the appropriate data interface, such as A1, A2, B1, or B2 |
| **IP Address** | Specifies the IP address. |
| **Public IP** | Specifies the public IP address. |
| **Gateway** | Specifies the gateway. |

### Related links

Configuring your network for the proxy service on page 432

# Retrieving Collaboration Agent, FMG, and WCS certificates and key files from the Avaya Aura® Conferencing system

You must obtain the Collaboration Agent, FMG, and WCS certificates from the Avaya Aura® Conferencing system by accessing the Element Manager administrative interface to retrieve the Collaboration Agent and FMG certificates and by directly accessing the WCS server to retrieve the WCS certificate.

### About this task

Use this task to retrieve the Collaboration Agent, FMG, and WCS certificates from your Avaya Aura® Conferencing system.

### Procedure

1. Retrieve the Collaboration Agent certificate.
    a. In the navigation pane of Element Manager Console, click **Security > Certificate Management > Keystore**.
    b. In the Keystore window, select the certificate you want to retrieve.
    c. Click **Export** to save the file locally.
    d. Select Keystore format **PKCS12 (p12)** and enter a password to encrypt the keystore.
    e. Click **Apply** to save the certificate file locally.

f. Use OpenSSL to convert this .p12 file to a certificate file (.cer) and key file (.key).

   To export the certificate file from the .p12 file:

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

   If this is version 6.3 of the SBC, the generated file is *.crt, so the command is:

   ```
   openssl pkcs12 -nokeys -clcerts -in filename.p12 -out filename.crt
   ```

   To export the key file from the .p12 file:

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

   For more information, see Introduction to certificates on page 552.

g. Enter your password if required.

   For p12 files, a password is always required.

2. Retrieve the FMG certificate.

   a. Access the FMG server using a terminal emulator, such as PuTTY to ensure secure access (SSH).

   b. Enter `su -` to log on as root.

   c. Navigate to `/var/mcp/run/fmg/certs`.

   d. Run `/usr/java/latest/bin/keytool -list -v -keystore FmgRtmps.jks` to list the contents of the FMG keystore.

   e. Run `/usr/java/latest/bin/keytool -importkeystore -srckeystore FmgRtmps.jks -destkeystore FmgRtmps.p12 -deststoretype PKCS12` to convert the format from jks to pkcs12.

   f. In the navigation pane of Element Manager Console, click **Security > Certificate Management > Keystore**.

   g. In the Keystore window, select the certificate you want to retrieve.

   h. Click **Export** to save the file locally.

   i. Select Keystore format **PKCS12 (p12)** and enter a password to encrypt the keystore.

   j. Click **Apply** to save the certificate file locally.

   k. Use OpenSSL to convert this .p12 file to a certificate file (.cer) and key file (.key).

      To export the certificate file from the .p12 file:

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

      If this is version 6.3 of the SBC, the generated file is *.crt, so the command is:

      ```
      openssl pkcs12 -nokeys -clcerts -in filename.p12 -out filename.crt
      ```

      To export the key file from the .p12 file:

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

      For more information, see Introduction to certificates on page 552.

   l. Enter your password if required.

      For p12 files, a password is always required.

3. Retrieve the WCS certificate.
    a. Access the WCS server using a terminal emulator, such as PuTTY to ensure secure access (SSH).
    b. Navigate to `/var/mcp/run/MCP_18.X/WCS1_0/certs`.
    c. Obtain two files and save them locally.
        - external.crt
        - external.key
4. Make a note of the location where you save the retrieved files.

**Related links**

Configuring Avaya Session Border Controller for Enterprise as a reverse proxy on page 427

# Retrieving the System Manager CA certificate

## Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. On the CA Functions page click **Download pem file**.
4. Click **Save** to save the certificate to a file.

**Related links**

Configuring Avaya Session Border Controller for Enterprise as a reverse proxy on page 427

# Installing the System Manager CA certificate

## About this task

You must add the System Manager root CA certificate, which you have just retrieved from System Manager, to the Avaya SBCE.

## Before you begin

- Retrieve the System Manager CA certificate from System Manager.
- Log into Avaya SBCE.

## Procedure

1. In the left navigation pane, click **TLS Management** > **Certificates**.
2. Click **Install**.
3. In the **Type** field, select **CA Certificate**.
4. In the **Name** field, type a name for the certificate.

5. Click **Browse** to locate the certificate file.
6. Click **Upload**.

**Related links**

Configuring Avaya Session Border Controller for Enterprise as a reverse proxy on page 427

## Installing the Collaboration Agent, WCS, and FMG certificates

You must add the Collaboration Agent and WCS certificates, which you have just retrieved, to the Avaya SBCE.

### About this task

You must add the Collaboration Agent, WCS, and FMG certificates, which you have just retrieved, to the Avaya SBCE. You must use this procedure to browse to the certificate files. You must perform this procedure three times because there are three separate certificates.

### Before you begin

- Retrieve the Collaboration Agent, WCS, and FMG certificates from the Avaya Aura® Conferencing system.
- Log into Avaya SBCE.

### Procedure

1. In the left navigation pane, click **TLS Management** > **Certificates**.
2. Click **Install**.
3. In the **Type** field, select **Certificate**.
4. In the **Name** field, type the name of the Certificate file.

   **Note:**

   You can type only letters, numbers, and underscores in the **Name** field. Enter the name of the Certificate file that is uploaded to the EMS. If the name of the Certificate file that you browse for uploading has a different name, that name will be changed with the Certificate name that is uploaded to the EMS.
5. In the **Certificate File** field, click **Browse** and browse to the location of the Certificate file.
6. In the **Key** field, select one of the following options:
   - **Use Existing Key from Filesystem**: Select this option if you generated a CSR from the Generate CSR screen. In this option, the key file is already in the correct location on the EMS.

     **Note:**

     If you are using this option, ensure that the Common Name in the Generate CSR screen matches with the name of the install certificate.
   - **Upload Key File**: Select this option if you generated a CSR by using an alternate method than the built-in Generate CSR screen.

In this option, you must upload the private key as described in Step 7.

7. **(Optional)** In the **Key File** field, click **Browse** and browse to the location of the key file
8. In the **Trust Chain File** field, click **Browse** and browse to the location of the trust chain file.

   This step is required if the CA provided a separate certificate trust chain.

   If the third party CA provides separate Root CA and Intermediate certificates, you must combine both files into a single certificate file for Avaya SBCE. To combine the files, add the contents of each certificate file one after the other, with the root certificate at the end.
9. Click **Upload**.
10. **(Optional)** If the SBC is not resident with the EMS, you must run some additional commands.
    a. Using a terminal emulator, such as PuTTY, SSH by way of port 222 to the Management IP of the SBC application server.
    b. Run the following commands:

    ```
    clipcs
    certsync
    ```
11. Repeat these steps for the additional certificates. For example, if you installed the Collaboration Agent certificate, you must now install the WCS or FMG certificate.

### Result

Avaya SBCE installs the Collaboration Agent, WCS. and FMG certificates.

**Related links**

Configuring Avaya Session Border Controller for Enterprise as a reverse proxy on page 427
Install Certificate screen field descriptions on page 437

## Install Certificate screen field descriptions

| Name | Description |
|---|---|
| **Type** | The type of certificate that you want to install.<br>Options are: **Certificate**, **CA Certificate**, or **Certificate Revocation List**. |
| **Name** | The name of the certificate that you want to install.<br>This field is optional, and if not specified, the filename of the uploaded certificate is used as the certificate name. Additionally, specifying a name same as another certificate will overwrite the existing certificate with the one being uploaded. |
| **Certificate File** | The location of the certificate on your system. Depending on your browser, click **Browse** or **Choose file** to browse for the file.<br>If the third party CA provides separate Root CA and Intermediate certificates, you must combine both files into a single certificate file for Avaya SBCE. To combine the files, add the contents of each certificate file one after the other, with the root certificate at the end. |

*Table continues…*

| Name | Description |
|---|---|
| **Trust Chain File** | The trust chain file used to verify the authenticity of the certificate. Depending on the browser, click **Browse** or **Choose File** to locate the file. |
| **Key** | The private key that you want to use. You can opt to use the existing key or select a file containing another key. |
| **Key File** | The button that is displayed when you select **Upload Key File** in the **Key** field. Depending on the browser, click **Browse** or **Choose File** to locate the file. |

**Related links**

Installing the Collaboration Agent, WCS, and FMG certificates on page 436

## Creating client profiles for the Collaboration Agent, WCS, and FMG

A Client Profile is used where the Avaya SBCE starts an outgoing connection towards a remote entity over TLS, such as a call server.

You must create three client profiles: One for the Collaboration Agent, one for the WCS, and one for the FMG. For the Collaboration Agent client profile, select the Collaboration Agent certificate, which you just retrieved and installed. For the WCS client profile, select the WCS certificate, which you just retrieved and installed. For the FMG client profile, select the FMG certificate, which you just retrieved and installed. In each case, the **Peer Certificate Authorities** should be the Avaya SBCE certificate and the System Manager CA certificate, which you just retrieved and installed. For example, AvayaSBCCA.crt and SMGR137_0402.cer. In each case, **Ciphers** should be set to **All**.

Set **Verification Depth** to 1.

**Related links**

Configuring Avaya Session Border Controller for Enterprise as a reverse proxy on page 427
Creating a client profile on page 438
TLS client profile screen field descriptions on page 439

### Creating a client profile

#### Procedure

1. Log in to Avaya SBCE EMS web interface with administrator credentials.
2. In the left navigation pane, click **TLS Management** > **Client Profiles**.
3. Click **Add**.

   The system displays the **New Profile** window.
4. Enter the requested information in the appropriate fields.

   For the Collaboration Agent client profile, select the Collaboration Agent certificate, which you just retrieved and installed. For the WCS client profile, select the WCS certificate, which you just retrieved and installed. For the FMG client profile, select the FMG certificate, which you just retrieved and installed. In each case, the **Peer Certificate Authorities** should be the Avaya SBCE certificate and the System Manager CA certificate, which you just retrieved and installed. For example, AvayaSBCCA.crt and SMGR137_0402.cer. In each case, **Ciphers** should be set to **All**.

5. Click **Finish**.

   The system installs and displays the new TLS client profile.

**Related links**

Creating client profiles for the Collaboration Agent, WCS, and FMG on page 438

## TLS client profile screen field descriptions

Both TLS Server Profiles and TLS Client Profiles share the same configuration parameters. Therefore, the parameter descriptions in the following table match those in the table in TLS server profile pop-up window field descriptions on page 442.

**Note:**

The only exception is regarding the Peer Verification parameter setting. This setting determines whether a peer verification operation must be performed. In a TLS client profile, the Peer Verification parameter setting cannot be changed and is locked to: **Required**. In a TLS server profile, the Peer Verification parameter can be set to one of three possible values: **Required**, **Optional**,or **None**.

| Name | Description |
|---|---|
| **TLS Profile** | |
| **Profile Name** | A descriptive name used to identify this profile. |
| **Certificate** | The certificate presented when requested by a peer.<br>**Tip:**<br>For the client profile, you should select the default certificate of the Avaya SBCE. |
| Certificate Info | |
| **Peer Verification** | The incoming connection must provide a certificate, the certificate must be signed by one of the Peer Certificate Authorities, and not be contained in a Peer Certificate Revocation List. In a client profile configuration screen, the **Required** is selected for this field.<br>**Note:**<br>Peer Verification is always required for TLS Client Profiles, therefore the **Peer Certificate Authorities**, **Peer Certificate Revocation Lists**, and **Verification Depth** fields will be active. |
| **Peer Certificate Authorities** | The CA certificates to be used to verify the remote entity identity certificate, if one has been provided. |

*Table continues…*

| Name | Description |
|---|---|
| | **Note:**<br>Using **Ctrl** or **Ctrl+Shift**, any combination of selections can be made from this list.<br>Using **Ctrl+Shift** , the user can drag to select multiple lines, and using **Ctrl**, the user can click to toggle individual lines.<br>**Tip:**<br>The list of peer certificate authorities should contain certificates from the verification chain of the Collaboration Agent/WCS/FMG certificate. If the Collaboration Agent/WCS/FMG server uses certificates signed by System Manager, use the root certificate authority of System Manager. |
| **Peer Certificate Revocation Lists** | Revocation lists that are to be used to verify whether a peer certificate is valid.<br>**Note:**<br>Using **Ctrl** or **Ctrl+Shift**, any combination of selections can be made from this list.<br>Using **Ctrl+Shift** , the user can drag to select multiple lines, and using **Ctrl**, the user can click to toggle individual lines. |
| **Verification Depth** | The maximum depth used for the certificate trust chain verification. Each CA certificate might also have its own depth setting, referred to as the path length constraint. If both are set, the lower of these two values is used.<br>**Tip:**<br>Set **Verification Depth** to 1. |
| Renegotiation Parameters | |
| **Renegotiation Time** | The amount of time after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable. |
| **Renegotiation Byte Count** | The number of bytes after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable. |
| Handshake Options | |
| **Version** | The TLS versions that the client or servers accepts or offers.<br>The options are:<br>• TLS 1.2<br>• TLS 1.1<br>• TLS 1.0<br>The default value for this field is TLS 1.2. Ensure that you select an appropriate TLS version according to the TLS version that the client supports. |
| **Ciphers** | The level of security to be used for encrypting data. Available selections are:<br>• Default: The cipher suite recommended by Avaya.<br>• FIPS: The cipher suite recommended by Avaya for FIPS 140–2 compatibility. |

*Table continues…*

| Name | Description |
|---|---|
| | • Custom: Selecting the Custom radio button enables a user-defined level of encryption that can be configured by using the Value field described below. |
| **Value** | A field provided to contain a textual representation of the ciphers settings used by OpenSSL.<br>For a full list of possible values, see the OpenSSL ciphers documentation at http://www.openssl.org/docs/apps/ciphers.html.<br>**Note:**<br>The Value field is an advanced setting that must not be changed without an understanding of how OpenSSL handles ciphers. Invalid or incorrect settings in this field can cause insecure communications or even catastrophic failure. |

**Related links**

Creating client profiles for the Collaboration Agent, WCS, and FMG on page 438

## Creating server profiles for the Collaboration Agent, WCS, and FMG

A Server Profile is used where Avaya SBCE processes an incoming connection over TLS from a remote entity. For example, server profile is used while processing a connection from an endpoint.

You must create three server profiles: One for the Collaboration Agent, one for the WCS, and one for the FMG. For the Collaboration Agent server profile, select the Collaboration Agent certificate, which you just retrieved and installed. For the WCS server profile, select the WCS certificate, which you just retrieved and installed. For the FMG server profile, select the FMG certificate, which you just retrieved and installed. In each case, the **Peer Certificate Authorities** should be the Avaya SBCE certificate and the System Manager CA certificate, which you just retrieved and installed. For example, AvayaSBCCA.crt and SMGR137_0402.cer. In each case, **Ciphers** should be set to **All**.

For TLS Server Profiles of Collaboration Agent, WCS and FMG, set **Peer Verification** to **None**.

Set **Verification Depth** to 1.

**Related links**

Configuring Avaya Session Border Controller for Enterprise as a reverse proxy on page 427
Creating a new TLS server profile on page 441
TLS server profile screen field descriptions on page 442

## Creating a new TLS server profile

### Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **TLS Management** > **Server Profiles**.

The system displays the Server Profiles screen.

3. Click **Add**.

   The system displays the New Profile window.

4. Enter the requested information into the appropriate fields.

   For the Collaboration Agent server profile, select the Collaboration Agent certificate, which you just retrieved and installed. For the WCS server profile, select the WCS certificate, which you just retrieved and installed. For the FMG server profile, select the FMG certificate, which you just retrieved and installed. In each case, the **Peer Certificate Authorities** should be the Avaya SBCE certificate and the System Manager CA certificate, which you just retrieved and installed. For example, AvayaSBCCA.crt and SMGR137_0402.cer. In each case, **Ciphers** should be set to **All**.

   For TLS Server Profiles of Collaboration Agent, WCS and FMG, set **Peer Verification** to **None**.

   Set **Verification Depth** to 1.

5. Click **Finish**.

   The TLS Server profile is created, installed, and listed in the application pane.

**Related links**

Creating server profiles for the Collaboration Agent, WCS, and FMG on page 441

## TLS server profile screen field descriptions

Both TLS Server Profiles and TLS Client Profiles share the same configuration parameters. Therefore, the parameter descriptions in the following table match those in the table in TLS Client Profile Pop-up Screen Field Descriptions on page 439

**Note:**

The only exception is regarding the Peer Verification parameter setting (see description below). This setting determines if a peer verification operation should be performed. In a TLS client profile, the Peer Verification parameter setting cannot be changed and is locked to: **Required**, while in a TLS server profile, the Peer Verification parameter may be set to one of three possible values: **Required**, **Optional**, or **None**.

| Field | Description |
|---|---|
| TLS Profile | |
| **Profile Name** | The descriptive name used to identify this profile. |
| **Certificate** | The certificate presented when requested by a peer.<br>**Tip:**<br>For the server profile, you should select the appropriate certificate of the Collaboration Agent/WCS/FMG which you have previously installed. |
| Certificate Info | |

*Table continues…*

| Field | Description |
|---|---|
| **Peer Verification** | One of three check boxes indicating whether peer verification is required:<br>• Required: The incoming connection must provide a certificate, the certificate must be signed by one of the Peer Certificate Authorities, and not be contained in a Peer Certificate Revocation List. In a client profile configuration screen, the **Required** check box is a locked setting and cannot be deselected.<br>• Optional: The incoming connection may optionally provide a certificate. If a certificate is provided, but is not contained in the Peer Certificate Authority list, or is contained in a Peer Certificate Revocation List, the connection will be rejected.<br>• None: No peer verification will be performed.<br>**Note:**<br>Peer Verification is always required for TLS Client Profiles, therefore the **Peer Certificate Authorities**, **Peer Certificate Revocation Lists**, and **Verification Depth** fields will be active.<br>**Tip:**<br>For TLS Server Profiles of Collaboration Agent, WCS and FMG, set **Peer Verification** to **None**. |
| **Peer Certificate Authorities** | The CA certificates to be used to verify the remote entity identity certificate, if one has been provided.<br>**Note:**<br>Using **Ctrl** or **Ctrl+Shift**, any combination of selections can be made from this list.<br>Using **Ctrl+Shift** , the user can drag to select multiple lines, and using **Ctrl**, the user can click to toggle individual lines. |
| **Peer Certificate Revocation Lists** | Revocation lists that are to be used to verify whether or not a peer certificate is valid.<br>**Note:**<br>Using **Ctrl** or **Ctrl+Shift**, any combination of selections can be made from this list.<br>Using **Ctrl+Shift** , the user can drag to select multiple lines, and using **Ctrl**, the user can click to toggle individual lines. |
| **Verification Depth** | The maximum depth used for the certificate trust chain verification. Each CA certificate might also have its own depth setting, referred to as the path length constraint. If both are set, the lower of these two values is used.<br>**Tip:**<br>Set **Verification Depth** to 1. |
| Renegotiation Parameters | |

*Table continues…*

| Field | Description |
|---|---|
| **Renegotiation Time** | The amount of time after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable. |
| **Renegotiation Byte Count** | The amount of bytes after which the TLS connection must be renegotiated. This field is optional and must be set to 0 to disable. |
| Handshake Options | |
| **Version** | The TLS versions that the client or servers accepts or offers.<br>The options are:<br>• TLS 1.2<br>• TLS 1.1<br>• TLS 1.0<br>The default value for this field is TLS 1.2. Ensure that you select an appropriate TLS version according to the TLS version that the server supports. |
| **Ciphers** | The level of security to be used for encrypting data. Available selections are:<br>• Default: The cipher suite recommended by Avaya.<br>• FIPS: The cipher suite recommended by Avaya for FIPS 140–2 compatibility.<br>• Custom: Selecting the Custom radio button enables a user-defined level of encryption that can be configured by using the Value field described below. |
| **Value** | A field provided to contain a textual representation of the ciphers settings used by OpenSSL.<br>For a full list of possible values, see the OpenSSL ciphers documentation at http://www.openssl.org/docs/apps/ciphers.html.<br>**Note:**<br>The Value field is an advanced setting that must not be changed without an understanding of how OpenSSL handles ciphers. Invalid or incorrect settings in this field can cause insecure communications or even catastrophic failure. |

**Related links**

Creating server profiles for the Collaboration Agent, WCS, and FMG on page 441

## Creating a reverse proxy for the Collaboration Agent, WCS, and FMG

### About this task

You must create three reverse proxy services: One for the Collaboration Agent, one for the WCS, and one for the FMG.

### Before you begin

Note the internal interface address and the two external interface addresses which you previously configured. This information is now required.

### Procedure

1. Log into Avaya SBCE.
2. In the left navigation pane, click **Device Specific Settings** > **DMZ Services** > **Relay Services**.

   The system displays the Relay Services page.
3. In the **Reverse Proxy** tab, click **Add**.
4. On the Add Reverse Proxy Profile page, do the following:
   a. In the **Service Name** field, type the reverse proxy profile name. You can enter any name.

   b. Select the **Enabled** check box.

   c. In the **Listen IP** field, click the external SBC IP address. For the Collaboration Agent, this IP address is the external interface IP address for Collaboration Agent. Similarly, for the WCS, this IP address is the external interface IP address for WCS. For the FMG, this IP address is the external interface IP address for FMG.

   d. In the **Listen Port** field, type the port for remote workers. This should be 443.

   e. In the **Listen Protocol** field, select the protocol published towards remote workers. This should be HTTPS.

   f. In the **Listen TLS Profile** field, click the server profile you created. For the Collaboration Agent, select the Collaboration Agent server profile. For the WCS, select the WCS server profile. For the FMG, select the FMG server profile.

   g. In the **Server Protocol** field, click the protocol used for the Avaya SBCE server. This should be HTTPS.

   h. In the **Server TLS Profile** field, click the client profile that you created. For the Collaboration Agent, select the Collaboration Agent client profile. For the WCS, select the WCS client profile. For the FMG, select the FMG client profile.

   i. In the **Connect IP** field, click the IP address that Avaya SBCE must use for communicating with the servers. This is the internal interface IP address.

   j. Select the **Allow Web Sockets** check box.

   k. In the **Server Addresses** field, type the server IP address and port number using this format <IP/FQDN>:<port>. For the Collaboration Agent, enter the Collaboration Agent server IP or FQDN. For the WCS, enter the WCS IP or FQDN. For the FMG, enter the FMG IP or FQDN.
5. Repeat these steps for the additional servers. For example, if you configured the Collaboration Agent traffic, you must now configure the WCS or FMG traffic.

**Related links**

Configuring Avaya Session Border Controller for Enterprise as a reverse proxy on page 427

## Configuring the Flash policy for the WCS

### About this task

The Web Collaboration Server (WCS) uses Adobe Flash®. You must configure the Avaya SBCE to ensure that this WCS traffic is secure.

### Before you begin

Note the internal interface address and the two external interface addresses which you previously configured. This information is now required.

### Procedure

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

   The following endpoints support Presence Server configuration by using PPM Mapping:

   - Avaya one-X® Communicator for Windows: Release 6.2 SP 11 Patch 3.
   - 96x1 phones: Release 6.5.
   - Avaya Equinox for all platforms: Release 3.0.
3. On the Relay Services page, click **Application Relay** > **Add** and do the following:
   a. In the **Name** field, type the application relay name. You can enter any name.
   b. In the **Service Type** field, select HTTP.
   c. In the **Remote IP/FQDN** field, enter internal IP of the WCS server.

      **Note:**

      If the SBC is version 6.3, you must type **Remote Domain** or **Published Domain**. This step is not required if the SBC is version 7.0.
   d. In the **Remote Port** field, type the port number. This should be 843.
   e. In the **Remote Transport** field, select TCP.
   f. In the **Listen IP** field, select the external interface IP address for WCS.
   g. In the **Listen Port** field, type the port number. This should be 843.
   h. In the **Connect IP** field, select the internal interface IP address.
   i. In the **Listen Transport** field, select TCP.
4. Click **Finish**.

**Related links**

Configuring Avaya Session Border Controller for Enterprise as a reverse proxy on page 427

# Chapter 26: Configuring Avaya Aura® Conferencing for access by the public internet

## Configuring Avaya Aura® Conferencing mobile devices for access by the public internet

### Mobile devices

Users with mobile devices, such as smartphones, can attend conferences and collaborate with other conference attendees whilst on the move.

For this release of Avaya Aura® Conferencing, Avaya support two applications:

- Avaya Web Collaboration Agent for iOS
- Avaya Web Collaboration Agent for Android

These applications are available from the Apple iTunes Store and the Google Play Store, respectively.

In order to support mobile devices for access by the public internet, you must configure the Session Border Controller (SBC). The SBC is not required for access by mobile users who are using the internal enterprise network.

### External access for Avaya Aura® Conferencing mobile clients

If you wish to offer Avaya Aura® Conferencing to smartphone users, who are outside of the enterprise firewall and if the Avaya Aura® Media Server (MS) resides within the enterprise firewall, you must configure a Session Border Controller (SBC).

Avaya has tested and recommends the Avaya Session Border Controller for Enterprise (also known as the Sipera SBC) for use with smartphone access. Avaya Aura® Conferencing provides access for mobile smartphone users by way of:

- Avaya Web Collaboration Agent for iOS

- Avaya Web Collaboration Agent for Android

For the purposes of connectivity, these mobile clients act as a standard remote worker through the SBC.

**Note:**

If you wish to offer connectivity for remote workers, you must perform advanced configuration on the SBC.

In this scenario, the SBC is configured to match the user agent of the Avaya Aura® Conferencing mobile client. The SBC routes requests from the mobile client directly to the SIP application server which is configured as the call server. The SIP signaling from the Avaya Aura® Conferencing mobile client does not route through Avaya Aura®.

In this release, the Avaya Aura® Conferencing mobile clients do not support secure RTP (SRTP). It is possible to configure the SBC to support RTP for the external media for mobile clients and SRTP for the internal media for mobile clients. However, Avaya does not recommend this configuration because Avaya Aura® Conferencing falsely marks the user as secure because it is unaware of the insecure leg.

While Avaya Aura® Conferencing does not support SRTP, it does support TLS for signaling. Avaya recommends TLS. Avaya also recommends using a new internal and external IP address on the SBC, specifically for use by the Avaya Aura® Conferencing mobile clients.

**Note:**

You should install and configure the SBC to route external calls to Avaya Aura® before commencing these steps.

For a better user experience, configure the network DNS to route the domain names accessed by the mobile client to the following addresses:

- External IP address of Avaya SBCE when the call is made form an external network.
- Internal Application Server and Collaboration Agent IP addresses when the call is made form the internal network.

In this case, the user does not need to use separate addresses for calls, but can use a single FQDN for accessing the Application Server or Collaboration Agent from both internal and external networks.

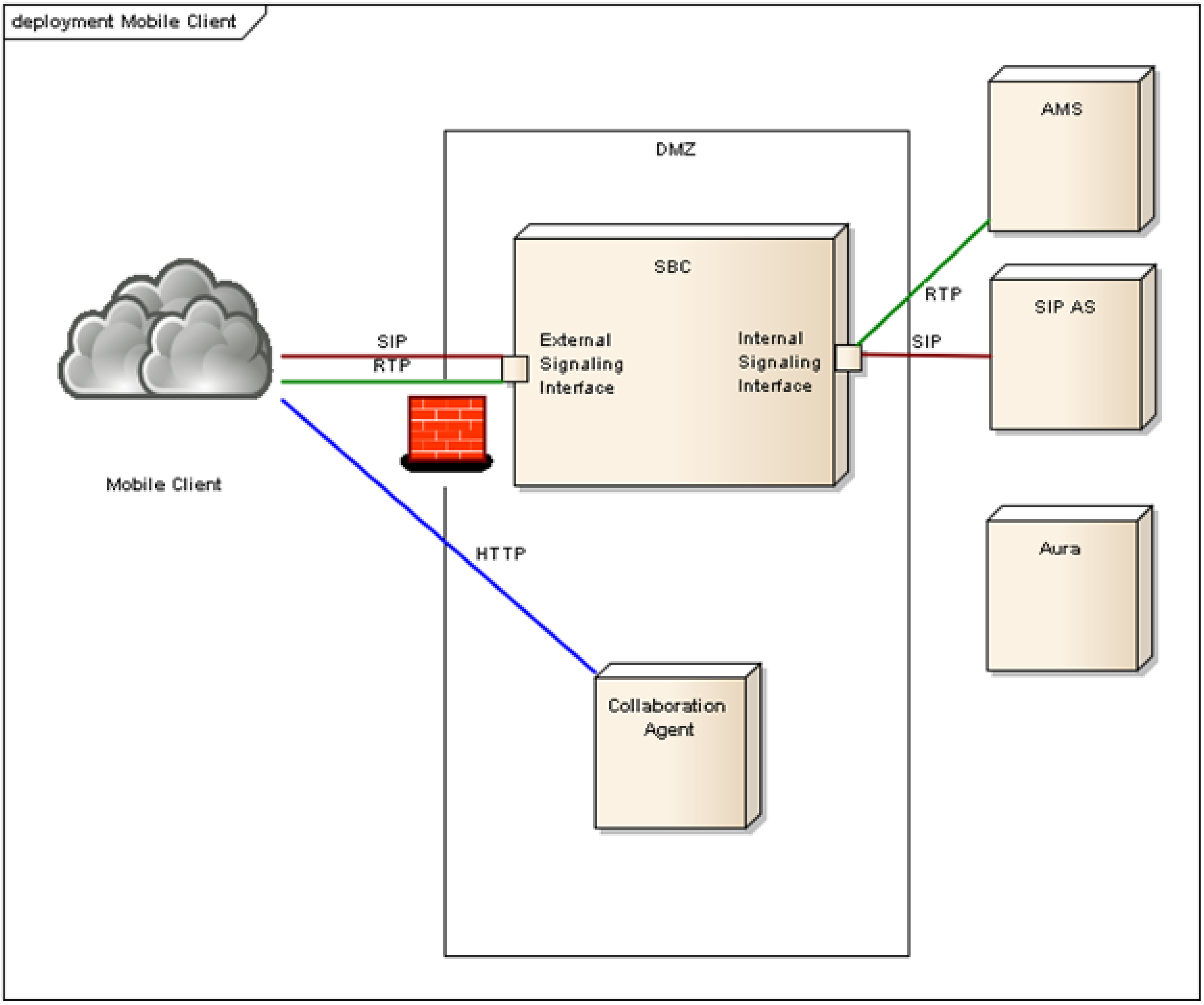


**Figure 26: Deployment of Avaya Aura® Conferencing to support mobile devices (Avaya Aura® deployment)**

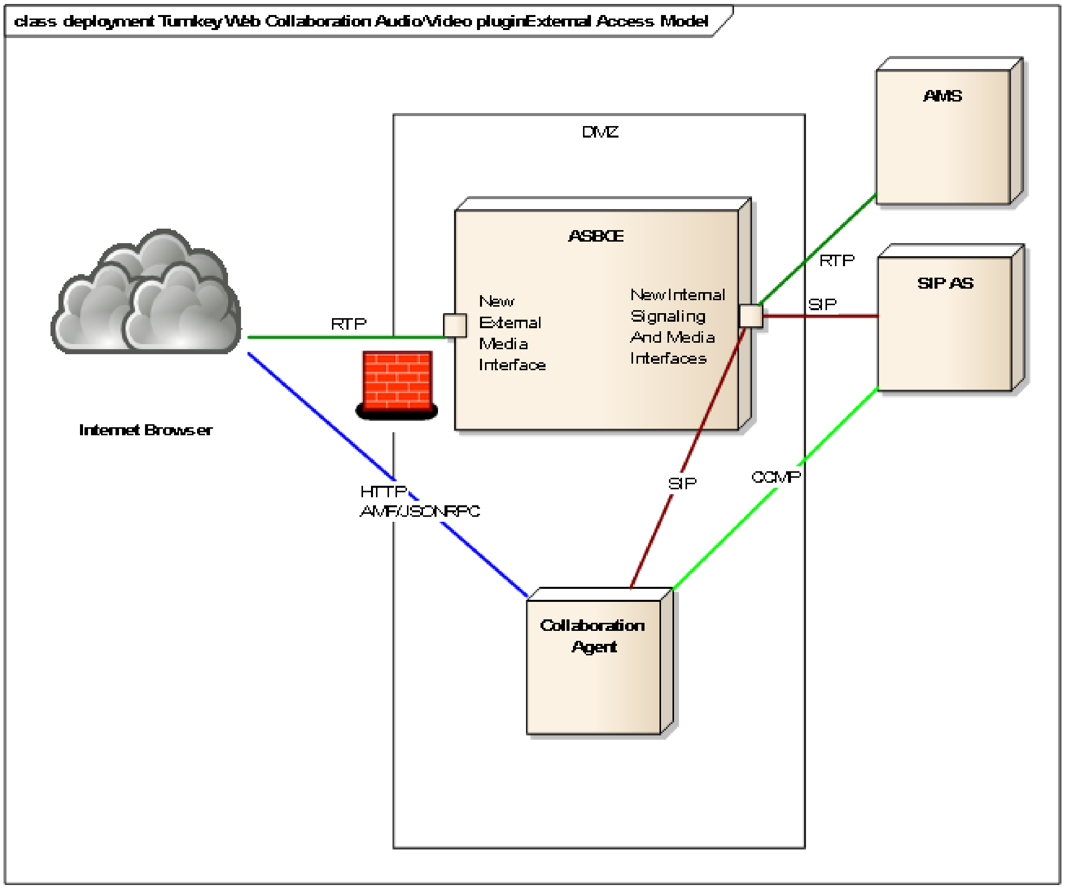

class deployment Turnkey Web Collaboration Audio/Video pluginExternal Access Model
DMZ
AMS
ASBCE
New External Media Interface
New Internal Signaling And Media Interfaces
RTP
SIP
SIP AS
RTP
Internet Browser
HTTP AMF/JSONRPC
SIP
CCMP
Collaboration Agent

**Figure 27: Deployment of Avaya Aura® Conferencing to support mobile devices (Turnkey deployment)**

## Checklist for mobile clients

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Download the Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager, and Avaya Aura® System Manager documentation from https://support.avaya.com/. | Avaya recommends the following:<br>• *Installing Avaya Session Border Controller for Enterprise*<br>• *Administering Avaya Session Border Controller for Enterprise*<br>• *Deploying Avaya Aura® Session Manager*<br>• *Administering Avaya Aura® Session Manager* | These documents do not apply in a Turnkey deployment. | |

*Table continues…*

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| | | • *Implementing Avaya Aura® System Manager on System Platform* | | |
| 2 | Add the Avaya Aura® System Manager Certificate Authority to the SBC. | Adding the Avaya Aura® System Manager Certificate Authority to the SBC on page 465 | These steps are not required if you are using TCP transport only. Avaya recommends TLS.<br>For a Turnkey deployment, Avaya recommends using OpenSSL for certificate signing requests. For more information, see Introduction to certificates on page 552. | |
| 3 | Create a TLS server profile. | Creating a Transport Layer Security (TLS) server profile on page 468 | | |
| 4 | Create a TLS client profile. | Creating a Transport Layer Security (TLS) client profile on page 469 | | |
| 5 | Create a server configuration for the Avaya Aura® Conferencing application server. | Creating a server configuration for the Avaya Aura® Conferencing application server on page 453 | | |
| 6 | Create an Avaya Aura® Conferencing application server routing profile. | Creating an Avaya Aura® Conferencing application server routing profile on page 454 | | |
| 7 | Create a user agent profile. | Creating a user agent profile on page 455 | | |
| 8 | Create a subscriber flow for Avaya Aura® Conferencing mobile clients. | Creating a subscriber flow for Avaya Aura® Conferencing mobile clients on page 455 | | |
| 9 | Create a server flow for the Avaya Aura® Conferencing application server. | Creating a server flow for the Avaya Aura® Conferencing application server on page 457 | | |

*Table continues…*

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 10 | Add the SBC as a trusted node in Element Manager. | Adding the SBC as a trusted node in Element Manager on page 459 | | |
| 11 | Ensure that the SBC location is served by a media server cluster. | Assigning a media server cluster to the SBC location on page 459 | | |
| 12 | Enable virtual register on the Avaya Aura® Conferencing application server. | Enabling virtual register on the Avaya Aura® Conferencing application server on page 460 | | |
| 13 | Ensure that the media port configuration on Avaya Aura® Conferencing matches the media port configuration on Avaya Session Border Controller for Enterprise. | Ensure that Avaya Aura Session Border Controller media interfaces port ranges correspond with Avaya Aura Conferencing media port ranges on page 458 | | |

**Tip:**

In the unlikely event that you experience any difficulties with this configuration, check Troubleshooting SBC connectivity issues on page 480.

## Creating a server configuration for the Avaya Aura® Conferencing application server

### Before you begin

Complete the steps in Creating a Transport Layer Security (TLS) client profile on page 469.

### About this task

Use this task to create a server configuration for the application server.

### Procedure

1. Login to the SBC EMS Web interface.
2. Navigate to **Global Profiles** > **Server Configuration**.
3. Click **Add**.
4. Enter a profile name and click **Next**.
5. Select **Call Server** as the server type.
6. Use the IP address of the Avaya Aura® Conferencing application server signaling address.
7. Select the supported transports and ports.

For secure configurations, select TLS and use port 5061.

For regular configurations, select TCP and use port 5060.

8. Do not check **Enable Authentication**.
9. Click **Next**.
10. Do not check **Enable Heartbeat**.
11. Click **Next**.
12. Select **Enable Grooming**.
13. **(Optional)** If you are using TLS, set the TLS Client Profile to the `aac` client profile.
14. Click **Finish**.

### Next steps

Refer back to the Checklist for mobile clients on page 451 to see the next task.

## Creating an Avaya Aura® Conferencing application server routing profile

### Before you begin

Complete the steps in Creating a server configuration for the Avaya Aura® Conferencing application server on page 453.

### About this task

Use this procedure to create a routing profile for an application server. For a better user experience, configure the network DNS to route the domain names accessed by the mobile client to the following addresses:

- External IP address of Avaya SBCE when the call is made form an external network.
- Internal Application Server and Collaboration Agent IP addresses when the call is made form the internal network.

### Procedure

1. Log in to the SBC EMS Web interface.
2. Navigate to **Global Profiles** > **Routing**.
3. Click **Add**.
4. Enter a profile name, such as `AAC-AppSvr`.
5. Click **Next**.
6. Use the ***** URI group.
7. In the **Next Hop Server1** panel, enter the Avaya Aura® Conferencing application server signaling address.

8. Select the supported transport.

   For secure configurations, select TLS.

   For regular configurations, select TCP.

9. Enter a Priority/Weight, such as 1.
10. Click **Finish**.

### Next steps

Refer back to the Checklist for mobile clients on page 451 to see the next task.

## Creating a user agent profile

### Before you begin

Complete the steps in Creating an Avaya Aura® Conferencing application server routing profile on page 454.

### About this task

Use this task to create a user agent profile.

### Procedure

1. Login to the SBC EMS Web interface.
2. Navigate to **Global Parameters** > **User Agents**.
3. Click **Add**.
4. Use the name `AACMobileUA`, or a similar preferred name.
5. Use the following regular expression, including the leading period and trailing asterisk:

   ```
   .*AvayaCollaborationApp.*
   ```

6. Click **Finish**.

### Next steps

Refer back to the Checklist for mobile clients on page 451 to see the next task.

## Creating a subscriber flow for Avaya Aura® Conferencing mobile clients

This flow represents the signaling from the mobile clients to the SBC external interfaces.

### Before you begin

Complete the steps in Creating a user agent profile on page 455.

### About this task

Use this task to create a subscriber flow.

## Procedure

1. Login to the SBC EMS Web interface.
2. Navigate to **Device Specific Settings** > **End Point Flows**.
3. Confirm that you are in the **Subscriber Flows** tab.
4. Click **Add**.
5. Enter a flow name, such as `AACMobileFlow`.
6. Select the user agent group that you created in Creating a user agent profile on page 455.
7. Leave the **URI Group**, **Subnet**, **Via Host**, and **Contact Host** as "`*`".
8. Select the expected external signaling interface.

   For example, `SBC_Ext_Sig1`.
9. Click **Next**.
10. Use **Subscriber** flow.
11. Use the expected external media interface.

    For example, `SBC_Ext_Media1`.
12. Select or clone the end point policy group, such as `default-low`.

    This profile provides a simple policy with defaults for RTP media and interworking.

    Avaya recommends cloning an existing policy group for the subscriber flow. If you use the default application policy, you will be limited in terms of the maximum number of concurrent sessions.

    **Tip:**

    Use the **Help** link on the SBC Web interface to learn more about this step.
13. Select the `AAC-AppSvr` routing profile.
14. For the **Interworking Profile**, select the Avaya-Ru profile.
15. For the **Topology Hiding Profile**, select the default profile.
16. If using TLS, use the aac TLS client that you created in Creating a Transport Layer Security (TLS) client profile on page 469.
17. Click **Finish**.

## Next steps

Refer back to the Checklist for mobile clients on page 451 to see the next task.

# Creating a server flow for the Avaya Aura® Conferencing application server

## Before you begin

Complete the steps in Creating a subscriber flow for Avaya Aura® Conferencing mobile clients on page 455.

## About this task

Use this task to create a server flow.

## Procedure

1. Login to the SBC EMS Web interface.
2. Navigate to **Device Specific Settings** > **End Point Flows**.
3. Tab to the **Server Flows** tab.
4. Click **Add**.
5. Enter a flow name, such as `AACServer Flow`.
6. Use the server configuration AAC that you defined in Creating a server configuration for the Avaya Aura® Conferencing application server on page 453.
7. For the **URI Group**, use "`*`".
8. Select the supported transport.

   For secure configurations, select TLS.

   For regular configurations, select TCP.
9. For the **Remote Subnet**, use "`*`".
10. For the **Received Interface**, (outgoing) **Signaling Interface**, and **Media Interface**, select the desired internal interface.

    For example:

    - Received interface: `SBC_Ext_Sig1`
    - Signaling interface: `SBC_Int_Sig1`
    - Media interface: `SBC_Int_Media1`
11. Select or clone the end point policy group, such as `default-low`.

    This profile provides a simple policy with defaults for RTP media and interworking.

    Avaya recommends cloning an existing policy group for the subscriber flow. You may need to modify the application policy to limit the number of sessions or update other rules, depending on your deployment.

**Tip:**

Use the **Help** link on the SBC Web interface to learn more about this step.

12. Select the `default` routing profile.
13. For the **Topology Hiding Profile**, select the default profile.
14. Click **Finish**.

### Next steps

Refer back to the Checklist for mobile clients on page 451 to see the next task.

## Ensure that Avaya Aura® Session Border Controller media interfaces port ranges correspond with Avaya Aura® Conferencing media port ranges

### About this task

Use this task to ensure that media ports configuration on Avaya Aura® Conferencing corresponds to the media ports configuration on Avaya Aura® Session Border Controller.

### Procedure

1. In the navigation pane of **Element Manager** Console, navigate to **Audio and Video Plugin** > **Port Settings** and make a note of the port range.
2. Navigate to **Feature Server Elements** > **Media Servers and Clusters**, choose a media server cluster and click **Media Ports Settings**.
3. Make a note of the port ranges configured for each cluster.
4. Log in to the SBC EMS Web interface.
5. Navigate to **Device Specific Settings** > **Media Interface**.
6. Check the port ranges configured for each internal and external interface and ensure that:
   - The external interface port ranges includes the port range configured in step 1.
   - The internal interface port ranges includes the port range configured in step 3.

   **Note:**

   Mobile client port ranges are not configured anywhere. Avaya recommends that mobile clients use 30000-40000 as the port range. External media interface port ranges should also include this port range.

# Adding the SBC as a trusted node in Element Manager

## Before you begin

Complete the steps in Creating a server flow for the Avaya Aura® Conferencing application server on page 457.

## About this task

Use this task to add the SBC as a trusted node in Avaya Aura® Conferencing Element Manager.

## Procedure

1. In the navigation pane of Element Manager Console, select **Addresses**.
2. Add the internal signaling IP address of the SBC to the **Addresses** list, using name such as `SBC1IntSigAddr`.
3. In the navigation pane of Element Manager Console, select **External Node**.
4. Under **External Nodes**, add a new node for the SBC, using name such as `SBC1IntSigNode`.
5. In the navigation pane of Element Manager Console, select **Session Border Controllers**.
6. Add an SBC, by clicking **Add (+-)**.
7. Enter a short name and a long name, such as `SBC1` and `SBC1`.
8. Select **Trusted**.
9. Select the SBC external node.
10. Select the supported transport.

    For secure configurations, select TLS.

    For regular configurations, select TCP.
11. Click **Apply**.

## Next steps

Refer back to the Checklist for mobile clients on page 451 to see the next task.

# Assigning a media server cluster to the SBC location

In order for the mobile devices to operate successfully, there must be a media server cluster serving the SBC location. If you do not assign a media server cluster to the SBC location, users will experience issues when they attempt to use the video conferencing feature on their mobile device.

## Before you begin

- Complete the steps in Adding the SBC as a trusted node in Element Manager on page 459.

- Log on to the Provisioning Client.

### About this task

Use this task to assign a media server cluster to the SBC location.

### Procedure

1. In the Provisioning Client window, navigate to **System Management** > **Routing** > **Session Border Controllers**.
2. On the **Session Border Controller Locations** tab, select an SBC for the selected location.
3. Click **Save**.
4. On the **Session Border Controller Physical Locations** tab, select a physical location for the selected SBC.
5. Click **Save**.

### Next steps

Refer back to the Checklist for mobile clients on page 451 to see the next task.

**Related links**

Assigning media server clusters to locations on page 319
Assigning media server clusters to a physical location on page 319

## Enabling virtual register on the Avaya Aura® Conferencing application server

### Before you begin

Complete the steps in Adding the SBC as a trusted node in Element Manager on page 459.

### About this task

Use this task to enable virtual register.

### Procedure

1. In the navigation pane of Element Manager Console, navigate to **Feature Server Elements** > **Application Servers** > **AS1** > **Configuration Parameters**.
2. Select the **VirtualRegistrar** Parm group.
3. Click **AllowRegistration** and **Edit (+-)**.
4. Change the value to **True**.
5. Click **Apply**.

# Deploying Avaya Web Collaboration audio and video plug-in for access by the public internet

If you wish to offer the Avaya Web Collaboration audio and video plug-in to users who reside outside of the enterprise firewall and if the Avaya Aura® Media Server (MS) resides within the enterprise firewall, you must configure a Session Border Controller (SBC). Avaya has tested and recommends the Avaya Session Border Controller for Enterprise (also known as the Sipera SBC) for use with the Avaya Web Collaboration audio and video plug-in.

You also require an SBC if you wish to offer the Avaya Web Collaboration audio and video plug-in to users who reside behind a Network Address Translation (NAT) hidden or private network.

**Note:**

You should install and configure the SBC to route external calls to Avaya Aura® before deploying Avaya Web Collaboration audio and video plug-in for external access. For more informations on installing the SBC, see Support for a Session Border Controller (SBC) on page 393.

### How Avaya Web Collaboration audio and video attempts to connect to the Avaya Aura® Media Server (MS)

When a conference user clicks the Avaya Web Collaboration audio and video on the Collaboration Agent interface, the Avaya Web Collaboration audio and video browser client initiates the following sequence:

- Firstly, the browser client attempts to connect directly to the Avaya Aura® Media Server (MS).
- If that fails, the browser client attempts to connect to the Avaya Aura® Media Server (MS) by way of the SBC that is assigned to the conference host location in the Avaya Aura® Conferencing Provisioning Manager. For more information, see Configuring location mapping for the plug-in on page 550.
- If that fails, for example if there is no SBC assigned to the conference host location, the browser client attempts to connect to the Avaya Aura® Media Server (MS) by way of the SBC that is assigned as the default SBC in the Avaya Aura® Conferencing Element Manager. For more information, see Adding the SBC to the Element Manager on page 476.
- If that fails, the browser client displays an error message to the conference user and denies them access to the feature.

### Avaya Web Collaboration audio and video in an Avaya Aura® deployment

In order to configure the Avaya Web Collaboration audio and video plug-in for use by external users, you must configure the Collaboration Agent server as a SIP trunk on the SBC. This means that it can send SIP signals to the Avaya Aura® System Manager from the Collaboration Agent.

For the incoming call flow:

- The signalling interface is an internal IP of the SBC.
- The media interface is an external IP.

For the outgoing call flow to the Avaya Aura® Session Manager:

- The signalling interface is the internal signalling interface.

- The media interface is the internal interface.

**Tip:**

Avaya recommends using a new internal and a new external IP on the Avaya Session Border Controller for Enterprise (SBC) for communications with the Avaya Web Collaboration audio and video plug-in. Use the **Help** link on the SBC Web interface to learn more about this task.

You must configure the SBC to Avaya Aura® Session Manager connection entity as a SIP trunk to the Avaya Aura® System Manager.

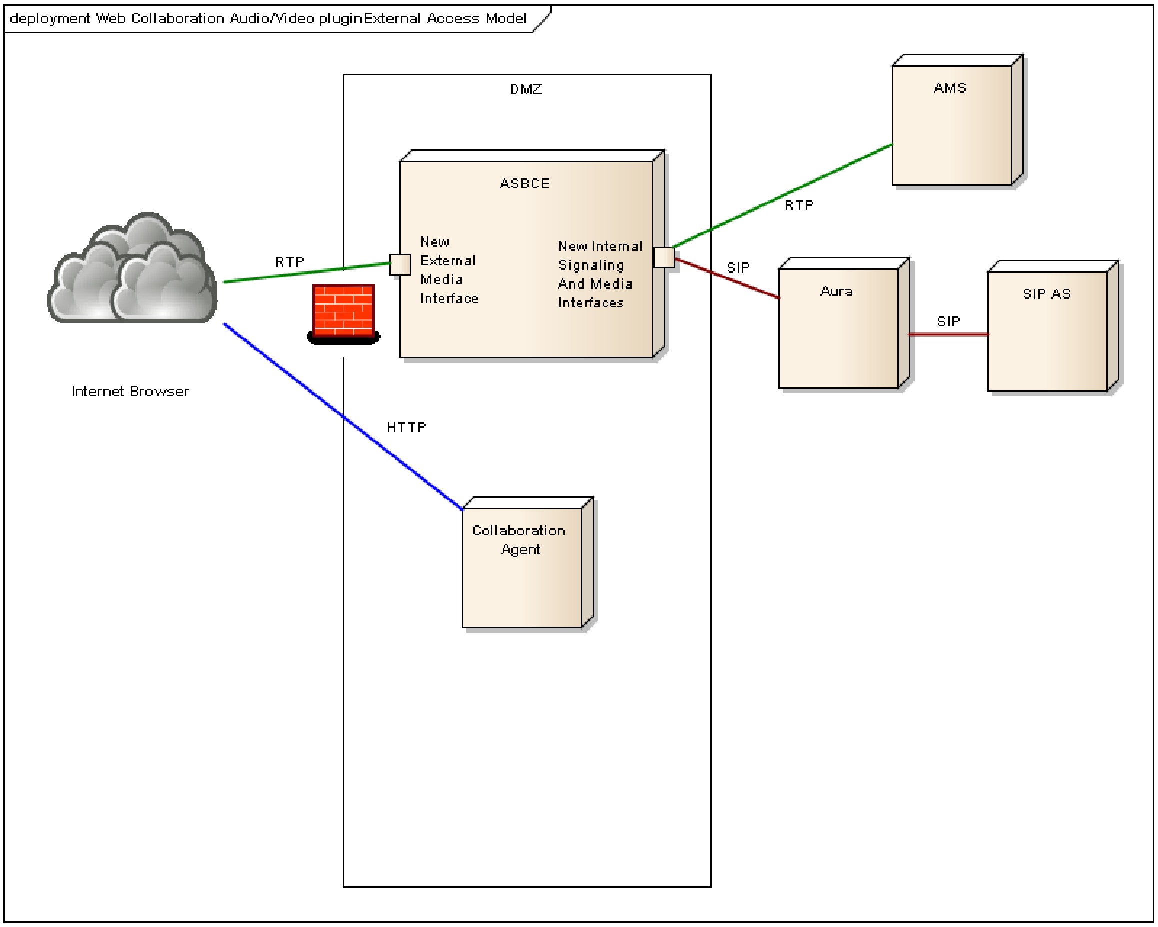

deployment Web Collaboration Audio/Video pluginExternal Access Model
DMZ
AMS
ASBCE
New External Media Interface
New Internal Signaling And Media Interfaces
RTP
RTP
SIP
Aura
SIP
SIP AS
Internet Browser
HTTP
Collaboration Agent

**Figure 28: Deployment of the Avaya Web Collaboration audio and video plug-in for external access (Avaya Aura® deployment)**

## Avaya Web Collaboration audio and video in a Turnkey deployment

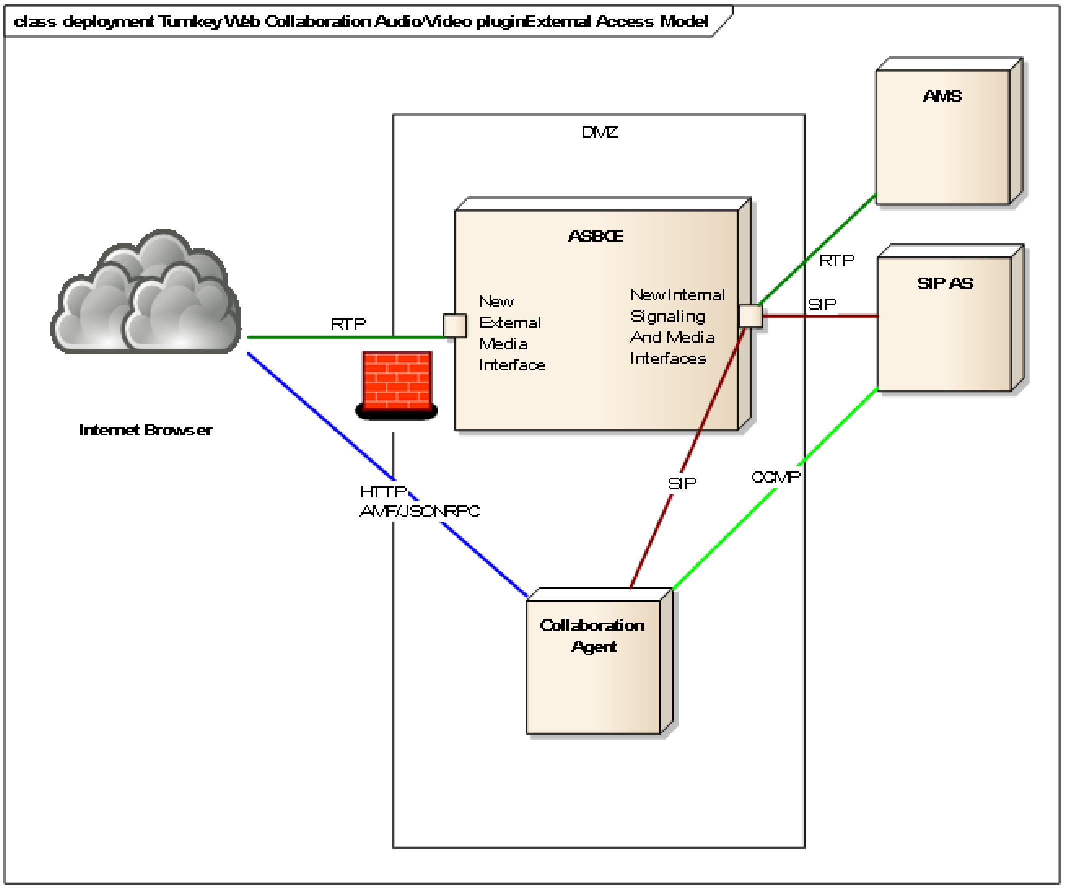

class deployment Turnkey Web Collaboration Audio/Video pluginExternal Access Model
DMZ
AMS
ASBCE
New External Media Interface
New Internal Signaling And Media Interfaces
RTP
SIP
SIP AS
RTP
Internet Browser
HTTP
AMF/JSONRPC
SIP
CCMP
Collaboration Agent

**Figure 29: Deployment of the Avaya Web Collaboration audio and video plug-in for external access (Turnkey deployment)**

### Related links

- Avaya Web Collaboration audio and video checklist on page 464
- Adding the Avaya Aura System Manager Certificate Authority to the SBC on page 465
- Installing the Collaboration Agent external and internal interface certificates on page 466
- Creating a Transport Layer Security (TLS) server profile on page 468
- Creating a Transport Layer Security (TLS) client profile on page 469
- Creating an interworking profile for the plug-in on page 469
- Configuring the Collaboration Agent as a trunk server on page 470
- Creating a Secure Realtime Transport Protocol-only (SRTP) media rule on page 471
- Adding the Collaboration Agent server flow on page 473
- Adding the internal interface Session Manager server flow on page 474
- Adding the SIP trunk to the Avaya Aura System Manager on page 475
- Adding the SBC to the Element Manager on page 476
- Assigning a default SBC in the Element Manager on page 477
- Configuring location settings for the SBC on page 478

Configuring ports on page 479
Troubleshooting SBC connectivity issues on page 480

## Avaya Web Collaboration audio and video checklist

In order to deploy the Avaya Web Collaboration audio and video plug-in, you must complete the following tasks.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Download the Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager, and Avaya Aura® System Manager documentation from https://support.avaya.com/. | Avaya recommends the following:<br>• *Installing Avaya Session Border Controller for Enterprise*<br>• *Administering Avaya Session Border Controller for Enterprise*<br>• *Deploying Avaya Aura® Session Manager*<br>• *Administering Avaya Aura® Session Manager*<br>• *Implementing Avaya Aura® System Manager on System Platform* | | |
| 2 | Add the Avaya Aura® System Manager Certificate Authority to the SBC. | Adding the Avaya Aura® System Manager Certificate Authority to the SBC on page 465 | | |
| 3 | Create a TLS server profile. | Creating a Transport Layer Security (TLS) server profile on page 468 | | |
| 4 | Create a TLS client profile. | Creating a Transport Layer Security (TLS) client profile on page 469 | | |
| 5 | Create an Interworking Profile for the Plug-in. | Creating an interworking profile for the plug-in on page 469 | | |
| 6 | Configure the Collaboration Agent as a trunk server. | Configuring the Collaboration Agent as a trunk server on page 470 | | |
| 7 | Create an SRTP-only media profile. | Creating a Secure Realtime Transport Protocol-only (SRTP) media rule on page 471 | | |
| 8 | Add the Collaboration Agent server flow. | Adding the Collaboration Agent server flow on page 473 | | |
| 9 | Add the internal interface Session Manager server flow. | Adding the internal interface Session Manager server flow on page 474 | | |
| 10 | Add the SIP trunk to Avaya Aura® System Manager. | Adding the SIP trunk to the Avaya Aura® System Manager on page 475 | | |
| 11 | Add the SBC to Element Manager. | Adding the SBC to the Element Manager on page 476 | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 12 | Assign a default SBC in Element Manager. | Assigning a default SBC in the Element Manager on page 477 | | |
| 13 | Configure the location details of the SBC in the Provisioning Client. | Configuring location settings for the SBC on page 478 | | |
| 14 | Ensure that the media port configuration on Avaya Aura® Conferencing matches the media port configuration on Avaya Session Border Controller for Enterprise. | Ensure that Avaya Aura Session Border Controller media interfaces port ranges correspond with Avaya Aura Conferencing media port ranges on page 458 | | |

**Tip:**

In the unlikely event that you experience any difficulties with this configuration, check Troubleshooting SBC connectivity issues on page 480.

**Related links**

Deploying Avaya Web Collaboration audio and video plug-in for access by the public internet on page 461

## Adding the Avaya Aura® System Manager Certificate Authority to the SBC

The Avaya Aura® System Manager Certificate Authority signs the certificates that Avaya Aura® Conferencing uses. As a result, you will first need to add the Avaya Aura® System Manager CA Certificate to the SBC trust store. You can obtain the Avaya Aura® System Manager Certificate Authority certificate from the Avaya Aura® System Manager Web interface **Security** tab.

These steps describe how to configure certificates for an Avaya Aura® deployment. For a Turnkey deployment, Avaya recommends that you use OpenSSL for certificate signing requests. For more information, see Introduction to certificates on page 552.

### About this task

Use this task to add the Avaya Aura® System Manager Certificate Authority to the SBC.

### Procedure

1. Login to the SBC EMS Web interface.
2. Navigate to **TLS Management** > **Certificates**.
3. Click **Install** to install the pem encoded certificate authority certificate from the Avaya Aura® System Manager.
4. Select CA Certificate under type.

5. Select a name, such as `smgrca`.
6. Click **Browse…** beside **Certificate File** and navigate to your pem encoded certificate authority certificate.
7. Click **Upload**.
8. **(Optional)** If the SBC is not resident with the EMS: Using a terminal emulator, such as PuTTY, SSH by way of port 222 to the Management IP of the SBC Application box and run the following commands:

   ```
   clipcs
   certsync
   ```

### Next steps

Refer back to your checklist to see the next task.

**Related links**

Deploying Avaya Web Collaboration audio and video plug-in for access by the public internet on page 461

## Installing the Collaboration Agent external and internal interface certificates

### About this task

You must add the certificates that you are planning to use for external access to the Collaboration Agent and for internal communication between the Collaboration Agent and Avaya SBCE.

The internal certificate is a client certificate that the Avaya SBCE uses to communicate with the Collaboration Agent. This certificate must match the IP address added to the Element Manager Console (EMS).

The external certificate is a client certificate that is used for external access to the Collaboration Agent. Starting from Avaya Aura® Conferencing Service Pack 10, this certificate must comply with the Avaya Aura® Conferencing certificate validation rules. For more information, see release notes for Avaya Aura® Conferencing Service Pack 10.

### Before you begin

Log in to the Avaya SBCE.

### Procedure

1. In the left navigation pane, click **TLS Management** > **Certificates**.
2. Click **Install**.
3. In the **Type** field, select **Certificate**.
4. In the **Name** field, enter the Certificate file name.

**Note:**

You can type only letters, numbers, and underscores in the **Name** field. Enter the name of the Certificate file that is uploaded to the EMS. If the Certificate file that you browse for uploading has a different name, Avaya Aura® Conferencingchanges that name with the Certificate file name that is uploaded to the EMS.

5. In the **Certificate File** field, click **Browse** and browse to the location of the Certificate file.
6. In the **Key** field, select one of the following options:
   - **Use Existing Key from Filesystem**: Select this option if you generated a CSR from the Generate CSR screen. In this option, the key file is already in the correct location on the EMS.

     **Note:**

     If you are using this option, ensure that the Common Name on the Generate CSR screen matches the name of the install certificate.
   - **Upload Key File**: Select this option if you generated a CSR by using an alternate method than the built-in Generate CSR screen.

     If you are using this option, you must upload the private key as described in Step 7.
7. **(Optional)** In the **Key File** field, click **Browse** and browse to the location of the key file.
8. In the **Trust Chain File** field, click **Browse** and browse to the location of the trust chain file.

   This step is required if the CA provided a separate certificate trust chain.

   If the third party CA provides separate Root CA and Intermediate certificates, you must combine both these files into a single certificate file for the Avaya SBCE. To combine this files, add the contents of each certificate file one after the other, with the root certificate at the end.
9. Click **Upload**.
10. **(Optional)** If the SBC is not resident with the EMS, do the following:
    a. Using a terminal emulation program, such as PuTTY, start a secure shell (SSH) connection to the Management IP of the SBC application server.

       Use port 222 to connect to the Avaya SBCE application server.

    b. Run the following commands:

```
clipcs
certsync
```

**Related links**

Deploying Avaya Web Collaboration audio and video plug-in for access by the public internet on page 461

## Creating a Transport Layer Security (TLS) server profile

This server profile represents the SBC acting as the server for the Avaya Aura® Conferencing Collaboration Agent. The SBC also acts as the server for the Avaya Aura® Conferencing application server and mobile clients. They must trust the SBC Certificate Authority. For the certificate prepared, you must first add its Certificate Authority (CA), such as the Avaya Aura® System Manager CA or a third party CA, to the Avaya SBCE. For more information, see Adding the Avaya Aura® System Manager Certificate Authority to the SBC on page 465.

### Before you begin

- Complete the steps in Adding the Avaya Aura® System Manager Certificate Authority to the SBC on page 465.
- Complete the steps in Installing the Collaboration Agent external and internal interface certificates on page 466.
- Log in to the Avaya SBCE.

### About this task

Use this task to create a TLS server profile.

### Procedure

1. Log in to the SBC EMS Web interface.
2. Navigate to **TLS Management** > **Server Profiles**.
3. Click **Add**.
4. Enter a server profile name such as `aac`.
5. Select the Collaboration Agent certificate for the external interface that you have installed.

   For more information, see Installing the Collaboration Agent external and internal interface certificates on page 466.
6. For **Peer Verification**, select **Optional**.
7. For **Peer Certificate Authorities**, select the Avaya Aura® System Manager Certificate Authority.
8. For **Verification Depth**, enter **1**.
9. For **Cipher**, select **Strong**.
10. Click **Finish**.

### Next steps

Refer back to your checklist to see the next task.

**Related links**

Deploying Avaya Web Collaboration audio and video plug-in for access by the public internet on page 461

## Creating a Transport Layer Security (TLS) client profile

This client profile represents the SBC acting as a client for the Avaya Aura® Conferencing Collaboration Agent. The SBC also acts as a client for the Avaya Aura® Conferencing SIP application server.

### Before you begin

Complete the steps in Creating a Transport Layer Security (TLS) server profile on page 468.

### About this task

Use this task to create a TLS client profile.

### Procedure

1. Log in to the SBC EMS Web interface.
2. Navigate to **TLS Management** > **Client Profiles**.
3. Click **Add**.
4. Enter a client profile name such as `aac`.
5. Select the Collaboration Agent certificate for the internal interface that you have installed.

   For more information, see Installing the Collaboration Agent external and internal interface certificates on page 466.
6. For **Peer Verification**, select **Required**.

   This forces mutual TLS when the SBC is a client of the Collaboration Agent.
7. For **Peer Certificate Authorities**, select the Avaya Aura® System Manager Certificate Authority.
8. For **Verification Depth**, enter **1**.
9. For **Cipher**, select **Strong**.
10. Click **Finish**.

### Next steps

Refer back to your checklist to see the next task.

**Related links**

Deploying Avaya Web Collaboration audio and video plug-in for access by the public internet on page 461

## Creating an interworking profile for the plug-in

### Before you begin

Complete the steps in Creating a Transport Layer Security (TLS) client profile on page 469.

### About this task

Use this task to create an interworking profile.

### Procedure

1. Login to the SBC EMS Web interface.
2. Navigate to **Global Profiles** > **Server Interworking**.
3. Select **avaya-ru**.
4. Click **Clone**.
5. Enter a name that you will easily remember, such as **avaya-ru-plugin**.
6. Click **Finish**.
7. Click the **Advanced** tab.
8. Click **Edit**.
9. Uncheck **Has Remote SBC**.
10. Click **Finish**.

### Next steps

Refer back to your checklist to see the next task.

#### Related links

Deploying Avaya Web Collaboration audio and video plug-in for access by the public internet on page 461

## Configuring the Collaboration Agent as a trunk server

### Before you begin

Complete the steps in Creating a Transport Layer Security (TLS) client profile on page 469.

### About this task

Use this task to configure the Collaboration Agent as a trunk server.

### Procedure

1. Login to the SBC EMS Web interface.
2. Navigate to **Global Profiles** > **Server Configuration**.
3. Click **Add**.
4. Enter a profile name, such as `AAC_CAs`.
5. Click **Next**.
6. For **Server Type** , select **Trunk Server**.

7. Enter the IP address of the Collaboration Agent, which is equivalent to the Collaboration Agent hosting server IP.

   The SIP signals are originating from the Collaboration Agent, so do **not** use the Avaya Aura® Conferencing application server signaling address.

8. Select **TLS** as the supported transport and use **TLS Port 5061** for secure configuration, otherwise.

   If you are using TCP transport, select **TCP** transport and **TCP Port 5060**.

9. Click **Next**.

10. Ensure that **Enable Authentication** is not checked.

11. Click **Next**.

12. Ensure that **Heartbeat** is not checked.

13. Click **Next**.

14. Select (or select a clone of) the `avaya-ru` interworking profile.

15. Select **Enable Grooming**, which allows for the TCP connection to be re-used for in-dialog messages.

    ✚ **Tip:**

    You can use the same server configuration for multiple Collaboration Agents, by adding comma delimited IPs of the Collaboration Agent.

### Next steps

Refer back to the Avaya Web Collaboration audio and video checklist on page 464 to see the next task.

#### Related links

Deploying Avaya Web Collaboration audio and video plug-in for access by the public internet on page 461

## Creating a Secure Realtime Transport Protocol-only (SRTP) media rule

This is an optional step.

### Before you begin

Complete the steps in Configuring the Collaboration Agent as a trunk server on page 470.

### About this task

Use this task to create an SRTP-only media profile for the Avaya Web Collaboration audio and video plug-in.

## Procedure

1. Login to the SBC EMS Web interface.
2. Navigate to **Domain Policies** > **Media Rules**.
3. Clone or create a new media rule by clicking **Add**.
4. Enter a rule name such as `eavica_srtp_media`.
5. Click **Next**.
6. **(Optional)** If this is version 6.3 of the SBC: Select **Learn Media IP dynamically** as the **Media Rule**.
7. For both audio and video:
    a. Select `SRTP_AES_CM_128_HMAC_SHA1_80` as the Preferred Format 1.
    b. Do not select **Encrypted RTCP**.
    c. Select **Interworking**.
    d. Select **Capability Negotiation**.
8. Do not select **Media Silencing**.
9. Click **Next**.
10. Do not select **RTCP enabled**.
11. Click **Next**.
12. Do not select **Media BFCP**.
13. Click **Next**.
14. Do not select **Media FECC**.
15. Click **Finish**.
16. Apply the media rule to a end point policy group by cloning or creating a new group.

    ⊕ **Tip:**

    Use the **Help** link on the SBC Web interface to learn more about this step.

## Next steps

Refer back to the Avaya Web Collaboration audio and video checklist on page 464 to see the next task.

### Related links

Deploying Avaya Web Collaboration audio and video plug-in for access by the public internet on page 461

## Adding the Collaboration Agent server flow

### Before you begin

Complete the steps in Creating a Secure Realtime Transport Protocol-only (SRTP) media rule on page 471.

### About this task

Use this task to add the Collaboration Agent server flow.

### Procedure

1. Login to the SBC EMS Web interface.
2. Navigate to **Device Specific Settings** > **End Point Flows**.
3. Tab to **Server Flows**.
4. Click **Add**.
5. Enter a name for the server flow, such as `AAC_CA`.
6. Add a server flow for the Avaya Web Collaboration audio and video plug-in signaling from the Collaboration Agent on the SBC's designated *internal* interface and media on the designated *external* interface.
7. For the **Received Interface and Signaling Interface** field, select the designated **Internal Signaling Interface**.
8. For the **Media Interface** field, select the designated **External Media Interface**.
9. Select an endpoint policy group that matches your desired configuration.

   Avaya recommends creating a new end point policy group cloned from an existing one. If you use the default application policy, you will be limited in terms of the maximum number of concurrent sessions.

   The Avaya Web Collaboration audio and video plug-in supports secure RTP (SRTP) audio and video, or a combination. For SRTP configurations, the media profile should support `SRTP_AES_CM_128_HMAC_SHA1_80`.

   a. For RTP, use or clone the `default-low` policy group.
   b. For SRTP audio through the SBC and unsecure video, use or clone the `avaya-def-low-enc` endpoint policy group.
   c. For SRTP only, use the policy group that you created for Creating a Secure Realtime Transport Protocol-only (SRTP) media rule on page 471.

   **Tip:**

   Use the **Help** link on the SBC Web interface to learn more about this step.
10. Select the routing profile that points to the Avaya Aura® Session Manager or, if this is a Turnkey deployment, select the routing profile that points to Avaya Aura® Conferencing AAC.

11. For the **Topology Hiding Profile**, select None.

### Next steps

Refer back to the Avaya Web Collaboration audio and video checklist on page 464 to see the next task.

### Related links

Deploying Avaya Web Collaboration audio and video plug-in for access by the public internet on page 461

## Adding the internal interface Session Manager server flow

### Before you begin

Complete the steps in Adding the Collaboration Agent server flow on page 473.

### About this task

Use this task to add the internal interface Avaya Aura® Session Manager server flow. In this flow, media comes through the internal media interface. If this is a Turnkey deployment, use this task to add the internal interface Avaya Aura® ConferencingAAC server flow.

### Procedure

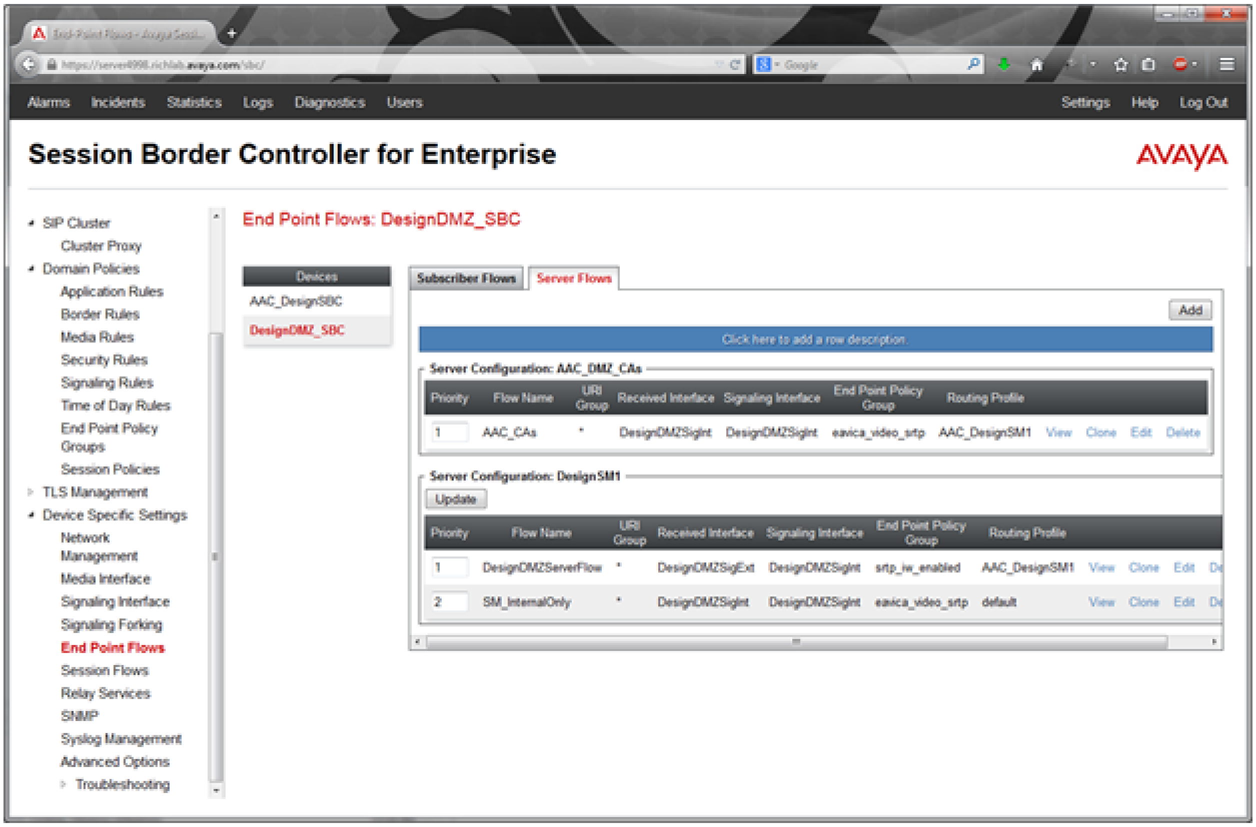
1. Login to the SBC EMS Web interface.
2. Navigate to **Device Specific Settings** > **End Point Flows**.
3. Tab to **Server Flows**.
4. Click **Add**.
5. Enter a name for the server flow, such as `SM_InternalOnly`.
6. Select the Avaya Aura® Session Manager server configuration.

   If this is a Turnkey deployment, select the Avaya Aura® Conferencing AAC server configuration.
7. For the **Received Interface and Signaling Interface** field, select the designated **Internal Signaling Interface**.
8. For the **Media Interface** field, select the designated **Internal Media Interface**.
9. Select an endpoint policy group that matches your desired configuration.

   This endpoint policy can be the same as the endpoint policy group that you selected for the Collaboration Agent server flow.
10. For the **Routing Profile**, select the default profile.
11. For the **Topology Hiding Profile**, select None.

### Example

Review your endpoint flow configuration. It should like similar to the following:



End Point Flows: DesignDMZ_SBC

Server Configuration: AAC_DMZ_CAs

| Priority | Flow Name | URI Group | Received Interface | Signaling Interface | End Point Policy Group | Routing Profile | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | AAC_CAs | * | DesignDMZSigInt | DesignDMZSigInt | eavica_video_srtp | AAC_DesignSM1 | View | Clone | Edit | Delete |

Server Configuration: DesignSM1

| Priority | Flow Name | URI Group | Received Interface | Signaling Interface | End Point Policy Group | Routing Profile | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | DesignDMZServerFlow | * | DesignDMZSigExt | DesignDMZSigInt | srtp_iw_enabled | AAC_DesignSM1 | View | Clone | Edit | De |
| 2 | SM_InternalOnly | * | DesignDMZSigInt | DesignDMZSigInt | eavica_video_srtp | default | View | Clone | Edit | De |

**Figure 30: Example Configuration**

### Next steps

Refer back to the Avaya Web Collaboration audio and video checklist on page 464 to see the next task.

#### Related links

Deploying Avaya Web Collaboration audio and video plug-in for access by the public internet on page 461

## Adding the SIP trunk to the Avaya Aura® System Manager

For more information about adding SIP trunks to Avaya Aura® System Manager, see Configuring the route to Avaya Aura® Conferencing on Avaya Aura® System Manager on page 309.

### Before you begin

Complete the steps in Adding the internal interface Session Manager server flow on page 474.

### About this task

Use this task to add the SBC to Avaya Aura® System Manager. If this is a Turnkey deployment, add the SBC to the appropriate node, such as CS1K, IP Office or directly to Communication Manager.

### Procedure

1. Log in to System Manager.
2. On the System Manager console, click **Elements** > **Routing**.
3. In the navigation pane, click **SIP Entities**.
4. On the SIP Entities page, click **New**.
5. Enter a new name, such as `SBC1`.
6. Add a new Sip Entity as a Sip Trunk
7. Create an entity link between the SBC and the Session Manager and over the desired port (TLS 5061 for secure, otherwise TCP 5060)

### Next steps

Refer back to the Avaya Web Collaboration audio and video checklist on page 464 to see the next task.

#### Related links

Deploying Avaya Web Collaboration audio and video plug-in for access by the public internet on page 461

## Adding the SBC to the Element Manager

The Avaya Session Border Controller for Enterprise is also known as the Sipera SBC.

### Before you begin

Complete the steps in Adding the SIP trunk to the Avaya Aura® System Manager on page 475.

### About this task

Use this task to add a default SBC to the Element Manager Console.

### Procedure

1. In the navigation pane of Element Manager Console, click **Addresses**.
2. In the Addresses window, click **Add (+)**.
3. In the Add IPv4 Address dialog box, enter the SBC Internal Signaling IP Address, using name such as `SBC1IntSigAddr`.
4. Click **Apply**.
5. In the navigation pane of Element Manager Console, select **External Nodes**.
6. In the External Nodes window, click **Add (+)**.
7. In the Add External Node dialog box, complete the following fields:
    - **Logical Name**: Type a logical name for the SBC, such as `SBC1IntSigNode`.
    - **IPv4 Address**: Type the IP address for the SBC.

8. Click **Apply**.
9. In the navigation pane of Element Manager Console, navigate to **Session Border Controllers** > **SBC Entity**.
10. In the **SBC Entity** window, click **Add (+)**.
11. In the Add SBC Entity dialog box, complete the following fields:
    - **Short Name**: Type a short name for the SBC
    - **Long Name**: Type a longer name for the SBC.
    - **Trusted**: Enable this checkbox.
    - **ExemptDosProtection**: Enable this checkbox.
    - **Perform Monitoring**: Do not enable this checkbox.
    - **Node**: Select the SBC defined in the **External Nodes** section of the Element Manager Console.
    - **Enable SIP TCP Port**: If you are using TLS, do not enable this checkbox. If you are using TCP, enable this checkbox.
    - **SIP TCP Port**: Enter 5060
    - **Enable SIP TLS Port**: If you are using TCP, do not enable this checkbox. If you are using TLS, enable this checkbox.
    - **SIP TLS Port**: Enter 5061.
12. Click **Apply**.

### Next steps

Refer back to the Avaya Web Collaboration audio and video checklist on page 464 to see the next task.

**Related links**

Deploying Avaya Web Collaboration audio and video plug-in for access by the public internet on page 461

## Assigning a default SBC in the Element Manager

### Before you begin

Complete the steps in Adding the SBC to the Element Manager on page 476.

### About this task

Use this task to assign a default SBC in the Element Manager console. This ensures the routing of calls when the location does not have an assigned SBC or the location cannot be determined.

### Procedure

1. On the Element Manager Console, navigate to **Session Border Controllers** > **Default SBC**.

2. Select the desired SBC from the drop-down menu.

### Next steps

Refer back to the Avaya Web Collaboration audio and video checklist on page 464 to see the next task.

**Related links**

Deploying Avaya Web Collaboration audio and video plug-in for access by the public internet on page 461

## Configuring location settings for the SBC

After you add the SBC to the Element Manager, you must provide location and routing details to the Provisioning Manager. This step is required when routing to the default SBC is not desired for a particular location.

### Before you begin

Add the SBC to the Element Manager Console. For more information, see Adding the SBC to the Element Manager on page 476 and Assigning a default SBC in the Element Manager on page 477.

### About this task

Use this task to add location details for the Avaya Session Border Controller for Enterprise to the Provisioning Manager.

### Procedure

1. In the Provisioning Client window, navigate to **System Management** > **Routing** > **Session Border Controllers**.
2. On the **Session Border Controller Locations** tab, from the **Select Location** drop-down list, select a location.
3. To assign SBCs to locations, copy the SBC from the **Available Session Border Controllers** box to the **Selected Session Border Controllers** box.
4. Click **Save**.
5. On the **Session Border Controller Physical Locations** tab, from the **Select Location** drop-down list, select a location.
6. To assign SBCs to locations, copy the SBC from the **Available Session Border Controllers** box to the **Selected Session Border Controllers** box.
7. Click **Save**.

**Related links**

Deploying Avaya Web Collaboration audio and video plug-in for access by the public internet on page 461

## Configuring ports

**Note:**

The Avaya Session Border Controller for Enterprise is also known as the Sipera SBC.

### About this task

Use this task to open the required firewall ports to enable the Avaya Web Collaboration audio and video plug-in to operate successfully.

### Procedure

1. On the Element Manager Console, navigate to **Audio and Video Plugin** > **Audio and Video Plugin Port Settings**.
2. On the **Audio and Video Plugin Port Settings** dialog, enter the UDP source port range entering the network to the SBC.
   a. In the **Start Port** field, enter `51,000`.
   b. In the **End Port** field, enter `53,000`.
3. Click **Apply**.

**Related links**

Deploying Avaya Web Collaboration audio and video plug-in for access by the public internet on page 461

Firewall ports on page 479

## Firewall ports

The following table shows the required firewall ports.

| Usage | Source network element | Destination network element | Protocol | Range |
|---|---|---|---|---|
| Sip connection | Collaboration Agent | Session Border Controller (SBC) private | TCP | 24053 |
| Sip connection | SBC private | Collaboration Agent | TCP | 5061 |
| Media | Avaya Web Collaboration audio and video plug-in | SBC public | UDP | 51,000–53,000 |

**Related links**

Configuring ports on page 479

## Troubleshooting SBC connectivity issues

- If the call is not going through, Avaya recommends looking at the **Incident Viewer** menu at the top left of the Avaya Session Border Controller for Enterprise interface.
- You can also log into the SBC and use the `traceSBC` command:
  1. Using a terminal emulator, such as PuTTY, SSH by way of port 222 to the Management IP of the SBC Application box.
  2. Log in as `ipcs`.
  3. Run the command `traceSBC –m`.
  4. Use `s` to start the capture or `f` to filter if this SBC is in use.
- If the previous methods of troubleshooting are not successful, you can use a packet capture to examine the issue in a pcap reader, such as Wireshark. A pcap reader provides network layer information and is useful for diagnosing TLS connection or firewall issues.
  1. In the SBC EMS Web interface, navigate to **Device Specific Settings** > **Advanced Options** > **Troubleshooting** > **Trace**.
  2. Select the SBC in question and tab to **Packet Capture**.
  3. Enter an appropriate capture filename and click **Start Capture**.
  4. Tab to **Captures** to download the packet capture.
- If the call is failing at the Avaya Aura® Session Manager (visible through an Avaya Aura® Session Manager trace), check the configuration of the SBC SIP Trunk on Avaya Aura® System Manager. If your deployment is a Turnkey deployment, check the configuration of the SBC SIP Trunk on Avaya Aura® Conferencing (AAC).

**Related links**

Deploying Avaya Web Collaboration audio and video plug-in for access by the public internet on page 461

# Chapter 27: Alarm and log forwarding to System Manager

## Enabling alarm forwarding to System Manager

### Before you begin

- You must have recorded the System Manager IP address, the Community, and TrapListener Port information from System Manager.
- You have created a logical name for System Manager.
- You have created an external node for System Manager.

### About this task

Use the following procedure to enable forwarding of Avaya Aura® Conferencing alarms as SNMP traps to System Manager by configuring and enabling an SNMP manager on Avaya Aura® Conferencing.

### Procedure

1. Log on to the Element Manager Console.
2. In the navigation pane, click **OAM Profiles** > **OSS Servers**.
3. Click **Add (+)**.
4. In the Add OSS Server dialog box, complete the following fields:
   - **Name**: Type a name, for example, SmgrOssServer.
   - **Node**: Choose **SmgrExtNode** from the list.
   - **Use External OAM Network**: Do not select this check box.
5. Click **Apply**.
6. In the navigation pane, click **OAM Profiles** > **SNMP Managers**.
7. Click **Add (+)**.
8. In the Add SNMP Manager dialog box, complete the following fields:
   - **Name**: Type a name, for example, SmgrSnmpManager.
   - **Community**: Type the community string as obtained from System Manager.
   - **Servers**: Select the server name you created in Step 4, for example, SmgrOssServer.

- **Trap Port**: Type the Trap Listener port number as obtained from System Manager.

9. Click **Apply**.
10. To restart Element Manager, perform the following:
    a. Log on to the server hosting EMServer instance 0 through ssh or the server console. At the logon prompt, type ntappadm or logon to an account with the AA role assigned.
    b. Type `./emStop.pl`, and press **Enter** to stop Element Manager.
    c. Type `./emStart.pl`, and press **Enter** to start Element Manager.
11. If you have a redundant instances of Element Manager, repeat Steps 1 through 10 for each instance.

## Disabling alarm forwarding to System Manager

### About this task

Use the following procedure to disable Avaya Aura® Conferencing alarm forwarding to System Manager.

### Procedure

1. Log on to the Element Manager Console.
2. In the navigation pane, click **OAM Profiles** > **SNMP Managers**.
3. Click **SmgrSnmpManager**, and click **Delete (-)** to delete the SNMP manager.
4. In the navigation pane, click **OAM Profiles** > **OSS Servers**.
5. Click **SmgrOssServer**, and click **Delete (-)** to delete the OSS server.
6. Restart Element Manager, perform the following:
    a. Navigate to **Feature Server Elements** > **Element Manager** > *<Element Manager NE>* > **NE Maintenance**.
    b. Select the EM instance to restart.
    c. Click **Restart**.
7. Log on to the server hosting EMServer instance 0 through ssh or the server console. At the logon prompt, type ntappadm or logon to an account with the AA role assigned.
    a. Type `./emStop.pl`, and press **Enter** to stop Element Manager.
    b. Type `./emStart.pl`, and press **Enter** to start Element Manager.
8. If you have a redundant instances of Element Manager, repeat Steps 1 through 7 for each instance.

# Checklist for forwarding logs to System Manager

The following checklist provides the high-level steps required to enable forwarding of the Avaya Aura® Conferencing logs to System Manager.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Review the prerequisites. | You have the following privileges:<br>• root access to Element Manager server<br>• access to the Element Manager Console<br>• access to System Manager | | |
| 2 | Generate enrollment password on System Manager and record information for future reference. | See Generating enrollment password on on page 483. | | |
| 4 | Configure Element Manager logs UDP transport client feed rule for forwarding to System Manager. | See Configuring Element Manager log UDP client feed rule on page 484. | | |
| 5 | Enable the logAgent to allow Element Manager logs to be forwarded to System Manager. A trust certificate is automatically installed in the SPIRIT agent for secure communication. | See Enabling log forwarding to on page 486. | | |

# Generating enrollment password on System Manager

## About this task

Use the following procedure to generate the enrollment password on System Manager.

## Procedure

1. Log on to System Manager.
2. On the System Manager console, click **Services** > **Security**.

3. In the navigation pane, click **Certificates**.
4. Click **Enrollment Password**.
5. In the **Password expires in** field, select **4 week(s)**.
6. In the **Password** field, type a new password.

   Record the FQDN or IP address and the enrollment password for future reference.
7. Click **Generate**.
8. Click **Commit**.

### Next steps

Proceed to configuring Element Manager log UDP client feed rule.

# Configuring Element Manager log UDP client feed rule

Element Manager logs can be sent to System Manager through the UDP transport to `/var/log/mcpacl`. The SPIRIT agent then forwards the logs to System Manager.

### About this task

Use this procedure to configure a log UDP client feed rule on Element Manager.

### Procedure

1. Log on to the Element Manager Console.
2. In the navigation pane of Element Manager Console, select **Addresses**.
3. In the Addresses window, click **Add (+)** .
4. In the Add IPv4 Address dialog box, complete the following fields:
   - **Logical Name**: Type `Localhost`.
   - **IPv4 Address**: Type `127.0.0.1`.
5. Click **Apply**.
6. In the navigation pane, click **External Nodes**.
7. In the External Nodes window, click **Add (+)** .
8. In the Add External Node dialog box, complete the following fields:
   - **Name**: Type `LocalhostNode`.
   - **IPv4 Address**: Select **Localhost** from the list.
9. Click **Apply**.
10. In the navigation pane, click **OSS Profiles** > **OSS Servers**.
11. In the OSS Servers window, click **Add (+)** .

12. In the Add OSS Server dialog box, complete the following fields:
    - **Name**: Type `LocalhostServer`.
    - **Node**: Select **LocalhostNode** from the list.
    - **Use External OAM Network**: Do not select the check box.
13. Click **Apply**.
14. In the navigation pane, click **OAM Profiles** > **OSS Endpoints**.
15. In the OSS Endpoints window, click **Add (+)** .
16. In the Add OSS Endpoint dialog box, complete the following fields:
    - **Name**: Type `Localhostsyslog`.
    - **Server**: Select **LocalhostServer**.
    - **Port**: Type `514`.
17. Click **Feature Server Elements** > **Element Manager** > **ElementManager** > **Log Processing** > **Log UDP Client Feed Rules**.
18. In the ElementManager Log UDP Client Feed Rules window, click **Add (+)** .
19. In the Add Log UDP Client Feed Rule dialog box, complete the following fields:
    - **Name**: Type `SecurityAuditSyslog`.
    - **Log Format**: Select **ACL**.
    - **Log Filter**: Select **security**.
    - **UDP Client Feed Rule**: Select the Localhostsyslog endpoint from the list on the left, and click **>>** to move to the list on the right.
20. Click **Apply**.
21. In the ElementManager Log UDP Client Feed Rules window, click **Add (+)** .
22. In the Add Log UDP Client Feed Rule dialog box, complete the following fields:
    - **Name**: Type `NonSecurityAuditSyslog`.
    - **Log Format**: Select **ACL**.
    - **Log Filter**: Select **NonSecurity**.
    - **UDP Client Feed Rule**: Select the Localhostsyslog endpoint from the list on the left, and click **>>** to move to the list on the right.
23. Click **Apply**.
24. In the navigation pane, click **Feature Server Elements** > **Element Manager** > **ElementManager** > **Log Processing** > **Log Rule Maintenance**.
25. In the ElementManager Log Processing Rules Maintenance window, click **Add (+)** .
26. Click the **UDP Client Feed** tab.

27. Click the name **SecurityAuditSyslog**, and click **Enable**.
28. Click the name **NonSecurityAuditSyslog**, and click **Enable**.
29. If you have a redundant instances of Element Manager, repeat Steps 17 through 28 for each instance.
30. On the **File** menu, click **Exit** to exit the Element Manager Console.

### Result

You have configured a log UDP client feed rule on Element Manager

### Next steps

Proceed to enabling log forwarding to System Manager.

## Enabling log forwarding to System Manager

### About this task

Use the following procedure to enable log forwarding to System Manager.

### Procedure

1. Log on to the Element Manager server as the root user.
2. Type **`logAgent enable <smgr-host> <smgr-port> <e-password>`**, and press **Enter**.

   where:

   - smgr-host is the FQDN or IP address of System Manager.
   - smgr-port is the https port of System Manager.
   - e-password is the enrollment password (unexpired).
3. If you have a redundant instances of Element Manager, repeat Steps 1 and 2 for each instance.

## Disabling log forwarding to System Manager

### About this task

Use the following procedure to disable log forwarding to System Manager.

### Procedure

1. Log on to the Element Manager server as the root user.
2. Type `logAgent disable`, and press **Enter**.

3. Log on to the Element Manager Console as admin.
4. In the navigation pane, click **Feature Server Elements** > **Element Manager** > **ElementManager** > **Log Processing** > **Log Rules Maintenance**.
5. Click the **UDP Client Feed** tab.
6. Click the line for SecurityAuditSyslog, and click **Disable**.
7. Click the line for NonSecurityAuditSyslog, and click **Disable**.
8. On the **File** menu, click **Exit** to exit the Element Manager Console.

# Chapter 28: Secure Access Link (SAL) gateway and external SNMP managers

## Secure Access Link Gateway overview

With Avaya Aura® Conferencing, the Secure Access Link (SAL) provides remote access to the Avaya Aura® Conferencing servers through SSH, to the Provisioning Manager using HTTPS, and to the Element Manager Graphical User Interface (GUI). SAL can also be configured to receive SNMP alarms from Avaya Aura® Conferencing.

In terms of Simple Network Management Protocol (SNMP) support, Avaya Aura® Conferencing supports the SNMP v1 and SNMP v2c protocols.

Depending on the deployment layout, either the integrated System Manager SAL gateway or an external standalone SAL gateway can be used to manage the Avaya Aura® Conferencing solution. The System Manager integrated SAL gateway can be used to manage a maximum of 10 individual or a combination of instances of Session Managers and Avaya Aura® Conferencing elements. For deployments that exceed 10 Session Managers or Avaya Aura® Conferencing elements, an external SAL gateway must be used.

## Enabling alarm forwarding to the SAL gateway

### Before you begin

- You have recorded the Secure Access Link (SAL) gateway IP address, the Community, and TrapListener Port information from the SAL gateway.
- You have created a logical name for the SAL gateway IP address.
- You have created an external node for the SAL gateway

  **Note:**

  This is required in Step 4 of the following procedure.

## About this task

Use the following procedure to enable forwarding of Avaya Aura® Conferencing alarms as SNMP traps to the SAL gateway by configuring and enabling an SNMP manager on Avaya Aura® Conferencing.

## Procedure

1. Log on to the Element Manager Console.
2. In the navigation pane, select **OAM Profiles** > **OSS Servers**.
3. Click **Add (+)**.
4. In the **Add OSS Server** dialog box, complete the following fields:
   - **Name**: Type a name, for example, SALgwOssServer.
   - **Node**: Choose the external node that was previously created.
   - **Use External OAM Network**: Do not select this check box.
5. Click **Apply**.
6. In the navigation pane, click **OAM Profiles** > **SNMP Managers**.
7. Click **Add (+)**.
8. In the **Add SNMP Manager** dialog box, complete the following fields:
   - **Name**: Type a name, for example, SALgwSnmpManager.
   - **Community**: Type the community string as obtained from the SAL gateway.
   - **Servers**: Select the server name you created in Step 4, for example, SALgwOssServer.
   - **Trap Port**: Type the Trap Listener port number as obtained from SAL gateway.
9. Click **Apply**.
10. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Element Manager** > **Element Manager** > **Alarm Processing** > **SNMP Managers**.
11. Click **Add (+)**.
12. Select the SNMP manager you added in Step 8, for example, SALgwSnmpManager.
13. Click **Delete (-)**.
14. Click **Apply**.
15. To restart Element Manager, perform the following:
    1. Log on to the server hosting EMServer instance 0 through ssh or the server console. At the logon prompt, type `ntappadm` or logon to an account with the AA role assigned.
    2. Type `./emStop.pl`, and press **Enter** to stop Element Manager.
    3. Type `./emStart.pl`, and press **Enter** to start Element Manager.

# Disabling alarm forwarding to the SAL gateway

## About this task

Use the following procedure to disable Avaya Aura® Conferencing alarm forwarding to the Secure Access Link (SAL) gateway.

## Procedure

1. Log on to the Element Manager Console.
2. In the navigation pane, click **Feature Server Elements** > **Element Manager** > **Element Manager** > **Alarm Processing** > **SNMP Managers**.
3. Click **SALgwSnmpManager**, and click **Delete (-)**.
4. In the navigation pane, click **OAM Profiles** > **SNMP Managers**.
5. Click **SALgwSnmpManager**, and click **Delete (-)** to delete the SNMP manager.
6. In the navigation pane, click **OAM Profiles** > **OSS Servers**.
7. Click **SALgwOssServer**, and click **Delete (-)** to delete the OSS server.

# Support for an external SNMP manager

You can configure Avaya Aura® Conferencing to forward alarms to the SAL gateway, to Avaya Aura® System Manager, or to an external Simple Network Management Protocol (SNMP) manager.

If you choose to forward alarms to an external SNMP manager, you require the SNMP Management Information Base (MIB) file. The MIB file for Avaya Aura® Conferencing is called AVCONFERENCING-MIB.mib and is stored on the Avaya Aura® Conferencing DVD in the following location:

```
dvd_AAC_MCP_X.X.X.XX_XXXX-XX-XX-XXXX_coreApps.iso
        MCP_XX.X.X.XX_XXXX-XX-XX-XXXX.zip
                clientAPIs
                        mibs
                                AVCONFERENCING-MIB.mib
```

In terms of Simple Network Management Protocol (SNMP) support, Avaya Aura® Conferencing supports the SNMP v1 and SNMP v2c protocols.

## Best practice

The AVCONFERENCING-MIB.mib file contains over 1800 traps (alarms). There are a large number of traps because some alarms can be raised with different severity levels and there is a unique trap to clear each level of alarm severity. As a result, there are actually only about 400 alarms that Avaya Aura® Conferencing can theoretically raise.

Avaya Aura® Conferencing administrators should always monitor the external SNMP manager for traps. However, alarms that are not classed as “Clear” or “Warning” are of particular importance. They indicate an issue with the system.

“Clear” alarms end with the letter “C” and “Warning” alarms end with the pattern ‘WARNING*dd*r where *dd* is any two digits

# Enabling alarm forwarding to an external SNMP manager

## Before you begin

- You have created a logical name for the external SNMP manager IP address.
- You have created an external node for the external SNMP manager.

  **Note:**

  This is required in Step 4 of the following procedure.

## About this task

Use the following procedure to enable forwarding of Avaya Aura® Conferencing alarms as SNMP traps to an external SNMP manager.

## Procedure

1. Log on to the Element Manager Console.
2. In the navigation pane, select **OAM Profiles** > **OSS Servers**.
3. Click **Add (+)**.
4. In the **Add OSS Server** dialog box, complete the following fields:
   - **Name**: Type a name, for example, ExternalSnmpOss.
   - **Node**: Choose the external node that was previously created.
   - **Use External OAM Network**: Do not select this check box.
5. Click **Apply**.
6. In the navigation pane, click **OAM Profiles** > **SNMP Managers**.
7. Click **Add (+)**.
8. In the **Add SNMP Manager** dialog box, complete the following fields:
   - **Name**: Type a name, for example, ExternalSNMPManager.
   - **Community**: Type the community string as obtained from the external SNMP manager.
   - **Servers**: Select the server name you created in Step 4, for example, ExternalSnmpOss.
   - **Trap Port**: Type the Trap Listener port number as obtained from the external SNMP manager.
9. Click **Apply**.
10. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Element Manager** > **Element Manager** > **Alarm Processing** > **SNMP Managers**.

11. Click **Add (+)**.
12. Select the SNMP manager you added in Step 8, for example, ExternalSNMPManager.
13. Click **Apply**.
14. To restart Element Manager, perform the following:
    a. Log on to the server hosting EMServer instance 0 through ssh or the server console. At the logon prompt, type `ntappadm` or logon to an account with the AA role assigned.

    b. Type `./emStop.pl`, and press **Enter** to stop Element Manager.

    c. Type `./emStart.pl`, and press **Enter** to start Element Manager.

# Disabling alarm forwarding to an external SNMP manager

## About this task

Use the following procedure to disable Avaya Aura® Conferencing alarm forwarding to an external SNMP manager.

## Procedure

1. Log on to the Element Manager Console.
2. In the navigation pane, click **Feature Server Elements** > **Element Manager** > **Element Manager** > **Alarm Processing** > **SNMP Managers**.
3. Click the External SNMP Manager, for example, ExternalSnmpManager, and click **Delete (-)**.
4. In the navigation pane, click **OAM Profiles** > **SNMP Managers**.
5. Click the External SNMP Manager, for example, ExternalSnmpManager, and click **Delete (-)** to delete the SNMP manager.
6. In the navigation pane, click **OAM Profiles** > **OSS Servers**.
7. Click **ExternalSnmpOss**, and click **Delete (-)** to delete the OSS server.

# Chapter 29: Configuring Communication Manager system parameters

## Checklist for Communication Manager parameter settings

Avaya Aura® Conferencing requires specific settings be enabled for Communication Manager.

The following checklist identifies the parameters required for configuring the Communication Manager using the System Manager for Avaya Aura® Conferencing. For more information about configuring the following parameters, see *Administering Avaya Aura® System Manager*.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Verify or modify the following feature-related system parameters:<br>• Multimedia Call Handling (Basic)<br>• Multimedia Call Handling (Enhanced)<br>• Multimedia IP SIP Trunking<br>• Direct IP-IP Audio Connections<br>• IP Audio Hairpinning<br>• SIP Endpoint Managed Transfer | See Modifying system parameters on page 494. | | |
| 2 | Verify or modify the following for Signaling groups:<br>• Direct IP-IP Audio Connections<br>• Initial IP-IP Direct Media<br>• IP Audio Hairpinning<br>• DTMF over IP | See Modifying Signaling Groups on page 495. | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 3 | View or modify the following IP options system parameters:<br>• Intra-System IP DTMF Transmission Mode<br>• Override ip-codec-set for SIP direct-media connections | See Modifying IP options system parameters on page 496. | | |
| 4 | View or modify the following settings for each IP codec set:<br>• Allow Direct-IP Multimedia<br>• Maximum Call Rate for Direct-IP Multimedia<br>• Maximum Call Rate for Priority Direct-IP Multimedia | See Modifying IP codec sets on page 497. | | |

# Modifying Communication Manager system parameters

## About this task

Use the following procedure to verify or modify the system parameters.

## Procedure

1. Log on to System Manager as admin.
2. On the System Manager console, click **Elements >** Communication Manager.
3. In the navigation pane, click **Parameters > System Parameters – Customer Options**.
4. On the System Parameters – Customer Options screen, select the appropriate device, and click **View**.
5. Navigate to page 5.
6. On page 5, verify the following:
    - **Multimedia Call Handling (Basic)** is set to **Y**.
    - **Multimedia Call Handling (Enhanced)** is set to **Y**.
    - **Multimedia IP SIP Trunking** is set to **Y**.

    **Note:**

    If these system parameters are not set correctly, contact Avaya support.

7. In the navigation pane, click **Parameters > System Parameters – Features**.
8. On the System Parameters – Features screen, click **New**.
9. Click **Prev Page** to go to page 19.
10. In the IP Parameters section, verify or change the following:
    - **Direct IP-IP Audio Connections** to **Y**.
    - **IP Audio Hairpinning** to **N**.
    - **SIP Endpoint Managed Transfer** to **Y**.
11. Press **Enter** to save your changes.

### Result

You have verified or changed the IP parameters.

## Modifying Signaling Groups

### About this task

Use the following procedure to verify or modify the SIP direct media parameters.

### Procedure

1. Log on to System Manager as admin.
2. On the System Manager console, click **Elements > Communication Manager**.
3. In the navigation pane, click **Network > Signaling Groups**.
4. Click the check box of the appropriate signaling group, and then click **Edit**.
5. Verify or modify **Direct IP-IP Audio Connections** to **Y**.
6. Verify or modify **Initial IP-IP Direct Media** to **Y**.
7. Verify or modify **IP Audio Hairpinning** to **N**.
8. Verify or modify **DTMF over IP** to **rtp-payload**.
9. Repeat Steps 4 on page 495 to 8 on page 495 for the other group number, for example 128.

# Optional: Modifying IP network region for private numbering

### About this task

Use the following procedure to verify or modify private numbering. This procedure is optional if region 1 already exists.

### Procedure

1. Log on to System Manager as admin.
2. On the System Manager console, click **Elements** > **Communication Manager**.
3. In the navigation pane, click **Network** > **IP Network Regions**.
4. Click the option button for the appropriate region, and then click **Edit**.

### Result

The private numbering is verified or modified.

# Modifying IP options system parameters

### Before you begin

You must use the *init* Login ID for this procedure.

### About this task

Use the following procedure to view or modify the IP options system parameters.

### Procedure

1. Open your Web browser and in the Address bar, type the IP address for the Communication Manager System Management Interface (SMI).
2. At the Logon ID prompt, type `init`, and click **Logon**.
3. Type your password, and click **Logon**.
4. On the Administration menu, click **Native Configuration Manager**.
5. In the Server Login window, type your Logon ID, and click **OK**.
6. Type your password, and click **OK**.
7. In the Command field, type `change system-parameters ip-options`, and click **Send**.
8. On the IP-options system parameters page, click **NEXT PAGE** to navigate to page 2.
9. In the **Intra-System IP DTMF Transmission Mode** field, select **rtp-payload**.
10. In the **Override ip-codec-set for SIP direct-media connections** field, type **y**.

11. Click **Enter**.
12. Close the Native Configuration Manager window.
13. In the Communication Manager system Management Interface (SMI) window, click **Logoff**.
14. Click **Log Off**.

# Modifying IP codec sets

## About this task

Use the following procedure to view or modify the IP codec sets for Communication Manager.

## Procedure

1. Open your Web browser and in the Address bar, type the IP address for the Communication Manager System Management Interface (SMI).
2. At the Logon ID prompt, type your Logon ID, and click **Logon**.
3. Type your password, and click **Logon**.
4. On the Administration menu, click **Native Configuration Manager**.
5. In the Server Login window, type your Logon ID, and click **OK**.
6. Type your password, and click **OK**.
7. In the Command field, type `change ip-codec-set #`, where `#` is the IP codec set you want to modify, and click **Send**.
8. On the IP Codec Set page, click **NEXT PAGE** to navigate to page 2.
9. In the **Allow Direct-IP Multimedia** field, type **y**.
10. In the **Maximum Call Rate for Direct-IP Multimedia** field, type **15360**. This setting is necessary for video.
11. In the **Maximum Call Rate for Priority Direct-IP Multimedia** field, type **15360**. This setting is necessary for video.
12. Click **Enter**.
13. Repeat Steps 7 through 12 for each IP codec set.
14. When finished, close the Native Configuration Manager window.
15. In the Communication Manager system Management Interface (SMI) window, click **Logoff**.
16. Click **Log Off**.

# Chapter 30: Integrating Avaya Aura® Conferencing with LDAP directory servers

This chapter describes the procedures to configure Avaya Aura® Conferencing to synchronize its database with LDAP directory servers. The LDAP directory integration feature enables an enterprise administrator to regularly synchronize the Avaya Aura® Conferencing database with LDAP directories. When Avaya Aura® Conferencing is integrated with LDAP directory servers, the conferencing subscriber data is managed in the LDAP directory. When a user logs into Avaya Aura® Conferencing via Collaboration Agent or a mobile client, the user will be authenticated directly against the password in the LDAP directory.

**Note:**

Avaya Aura® Conferencing supports any directory server that supports LDAP (for example, Microsoft® Active Directory 2003 and 2008 and OpenLDAP).

**Related links**

Pre-deployment checklist for LDAP integration on page 499
LDAP integration tasks on page 499
Configuring the physical sites on page 501
Configuring the IP addresses and ports for the directory servers on page 502
Adding the directory domains on page 503
Configuring directory servers on page 504
Configuring the directory synchronization service on page 506
Configuring the directory authentication service on page 510
Configuring the directory access passcode settings on page 510
Passcodes encryption on page 512
Configuring multiple directory domains on page 512
Configuring LDAP directory-synchronized users on System Manager on page 513
Retrieving the CA certificate from the Active Directory server on page 514
Assigning the Directory Server Certificate for the network elements on page 516

# Pre-deployment checklist for LDAP integration

The following checklist provides the high level steps and considerations prior to beginning your integration of Avaya Aura Conferencing with LDAP directory servers.

| # | Task | Notes | ✔ |
|---|---|---|---|
| 1 | Obtain the list of directory domains (including child domains or sub-domains) from which enterprise users will be added as Avaya Aura® Conferencing users. Examples of directory domains are `avaya.com`, `ca.avaya.com`, and `avaya.uk`. | | |
| 2 | Obtain the list of LDAP directory servers in each domain. For each directory server, you must have:<br>• IP address<br>• port<br>• connection credentials (user distinguished name and password) of a user with read access to the directory servers in the domain<br>• A maximum of two redundant servers for synchronization<br>• As many redundant servers as required for authentication. These servers can be the same redundant servers used for synchronization. | | |
| 3 | Obtain the list of physical sites in which the Avaya Aura® Conferencing network elements are deployed to determine the list of authentication servers the network elements will try. Examples of physical sites are `Enterprise Intranet` and `Enterprise DMZ`. | | |

**Related links**

Integrating Avaya Aura Conferencing with LDAP directory servers on page 498

# LDAP integration tasks

You must perform the following tasks to integrate Avaya Aura® Conferencing with LDAP directory servers.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Review the prerequisites. | See Pre-deployment checklist for LDAP integration on page 499. | | |
| 2 | Add each physical site in which Avaya Aura® Conferencing network elements are deployed, and assign these sites to the appropriate servers. | See Configuring the physical sites on page 501. | | |
| 3 | Add the IP address, add an external node, and configure the port for each directory server. | See Configuring the IP addresses and ports for the directory servers on page 502. | | |
| 4 | Add the directory domains that contain the enterprise users you want to add as Avaya Aura® Conferencing users. | See Adding the directory domains on page 503. | | |
| 5 | Configure the connection, synchronization, and authentication settings for the directory domains you added. | See Configuring directory servers on page 504. | | |
| 6 | Configure the directory synchronization service. | See Configuring the directory synchronization service on page 506. | | |
| 7 | Configure the timeout settings for directory authentication. | See Configuring the directory authentication service on page 510. | | |
| 8 | Configure the directory access passcode settings for each directory domain. | See Configuring the directory access passcode settings on page 510. | | |
| 9 | If you added multiple directory domains in Step 4, configure those additional directory domains. | See Configuring multiple directory domains on page 512. | | |
| 10 | Provision manually on Avaya Aura® System Manager each user that is synchronized from the LDAP directory. | See Configuring LDAP directory-synchronized users on System Manager on page 513. | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 11 | If you are using TLS to connect to the Active Directory server, retrieve the CA certificate from the Active Directory server. | See Retrieving the CA certificate from the Active Directory server on page 514. | | |

**Related links**

Integrating Avaya Aura Conferencing with LDAP directory servers on page 498

# Configuring the physical sites

## Before you begin

You must have the list of physical sites in which the Avaya Aura® Conferencing network elements are deployed.

## About this task

Use this procedure to add each physical site in which the Avaya Aura® Conferencing network elements are deployed and assign these sites to the appropriate servers.

## Procedure

1. In the navigation pane of Element Manager Console, select **Physical Sites**.
2. In the Physical Sites window, click **Add (+)**.
3. In the Add Site dialog box, complete the following fields:
   - **Name**: Enter a short name for the site (for example, `EnterIntranet`).
   - **Long Name**: Enter the full name for the site (for example, `EnterpriseIntranet`).
4. Click **Apply**.
5. Repeat Steps 2 through 4 for each physical site you want to configure.
6. In the navigation pane of Element Manager Console, click **Servers**.
7. In the Servers window, select **EMServer1**, and then click **Edit (-/+)**.
8. From the Physical Site box in the Edit Server dialog box, select the appropriate site you added in Steps 2 through 4.
9. Click **Apply**.
10. Repeat Steps 7 through 9 for each server displayed in the Servers window.
11. Click **Apply**.

**Related links**

Integrating Avaya Aura Conferencing with LDAP directory servers on page 498

# Configuring the IP addresses and ports for the directory servers

## Before you begin

For each directory server, you must know:

- the IP address
- whether the directory server is configured for secure access
- the port number

## About this task

Use this procedure to add the IP address, add an external node, and configure the port for each directory server.

## Procedure

1. In the navigation pane of Element Manager Console, click **Addresses**.
2. In the Addresses window, click **Add (+)**.
3. In the Add IPv4 Address dialog box, complete the following fields:
    - **Logical Name**: Type the logical name for the directory server (for example, `LDAP1`).
    - **IPv4 Address**: Type the IP address for the directory server.
4. Click **Apply**.
5. Repeat Steps 2 through 4 for each directory server.
6. In the navigation pane of Element Manager Console, select **External Nodes**.
7. In the External Nodes window, click **Add (+)**.
8. In the Add External Node dialog box, complete the following fields:
    - **Name**: Type a name for the directory server (for example, `LDAP1Node`).
    - **IPv4 Address**: Select the appropriate directory server address you added in Steps 2 through 4.
9. Click **Apply**.
10. Repeat Steps 7 through 9 for each directory server address you added in Steps 2 through 4.
11. In the navigation pane of Element Manager Console, click **Directory Access Servers**.
12. In the Directory Access Servers window, click **Add (+)**.
13. In the Add Directory Access Server dialog box, complete the following fields:
    - **Short Name**: Type the short name of the directory server (for example, `LDAP1`).
    - **Long Name**: Type the long name of the directory server (for example, `LDAPServer1`).

- **Node**: Select the directory server node you added previously (for example, **LDAP1Node**).
- **Enable TLS Port**: If the directory server is configured for secure access, select this check box. When this check box is selected, port 636 will be used by default. To change the port, enter the port you want to use.
- **Enable TCP Port**: If the directory server is configured for non-secure access, select this check box. When this check box is selected, port 389 will be used by default. To change the port, enter the port you want to use.

14. Click **Apply**.
15. Repeat Steps 11 through 13 for each directory server node you added in Steps 7 through 9.

**Note:**

If an LDAP directory server is configured with a TLS certificate that is signed by a non-System Manager Certificate Authority, you must export a copy of the Certificate Authority certificate and place the certificate in **Security > Truststore** in Element Manager Console. See Retrieving the CA certificate from the Active Directory server on page 514.

Optionally, if any of the directory servers are configured for mutual/client authentication, you must set the respective certificate/key in **Security > Keystore** in Element Manager Console to **Directory Server certificate** for the following network elements:

- Application Server
- Provisioning Manager
- Collaboration Agent Manager

To change the certificate/key to **Directory Server certificate** for these network elements, see Assigning the Directory Server Certificate for the network elements on page 516.

**Related links**

Integrating Avaya Aura Conferencing with LDAP directory servers on page 498

# Adding the directory domains

In order to successfully configure LDAP, you must create/add the LDAP domain in the **Enterprise Domains** tab.

### Before you begin

You must know the directory domains (including child domains or sub-domains) from which enterprise users will be added as Avaya Aura® Conferencing users.

### About this task

Use the following procedure to add the directory domains that contain the enterprise users you want to add as Avaya Aura® Conferencing users.

### Procedure

1. In the Provisioning Client window, select **System Management** > **User Domains**.
2. In the Enterprise Domain tab, enter the directory domain you want to add in the Enterprise Domain box.
3. Click **Add**.

   The directory domain appears at the bottom of the Enterprise Domain list.
4. Repeat Steps 2 and 3 for each directory domain you want to add.

**Related links**

Integrating Avaya Aura Conferencing with LDAP directory servers on page 498

## Configuring directory servers

### Before you begin

You must know the distinguished name and password of a user with read access to the directory servers in each domain (for example, `cn=administrator,cn=Users,dc=ca,dc=canada,dc=com`).

### About this task

Use the following procedure to configure the connection, synchronization, and authentication settings for the directory domains you added.

### Procedure

1. In the Provisioning Client window, select **System Management > Directory Access Services > Directory Servers**.
2. Click the **Connection Credentials** tab.
3. From the Select domain box, select the directory domain you want to configure. The Select domain box displays all the directory domains you have added.
4. In the Connection Principal box, enter the distinguished name of a user with read access to the directory servers in the selected domain (for example, `cn=administrator,cn=Users,dc=ca,dc=canada,dc=com`).
5. In the Connection Password box, enter the password of the user you entered in Step 4.
6. Click **Save**.
7. Click the **Synchronization Servers** tab.
8. From the Select domain box, select the directory domain you want to configure.

9. From the Primary Server box, select the primary server used for synchronization.
10. Perform one of the following steps:
    - If there is a redundant server, select the redundant server from the Secondary Server box.
    - If there is not a redundant server, select **Not Selected** from the Secondary Server box.
11. Click **Save**.
12. Click the **Authentication Servers** tab.
13. From the Select domain box, select the directory domain you want to configure.
14. From the Physical Site box, select the physical site of the Application Server or Provisioning Manager server. (Both of these servers usually reside together on your intranet.)
15. From the Authentication Server box, select the directory server that the Provisioning Manager server should try first for authentication for the domain.
16. Click **Add**.

    The information you entered appears at the top of the table.
17. Repeat Steps 14 through 16 for all other directory servers that the Provisioning Manager server can try for authentication for the domain.

    ✱ **Note:**

    The order in which the information is displayed in the table indicates the order in which the authentication servers are queried. Be sure to prioritize the list of authentication servers for each physical site based on availability or network access.
18. From the Physical Site box, select the physical site of Collaboration Agent Manager. (This site can reside in the DMZ.)
19. From the Authentication Server box, select the directory server that the Collaboration Agent Manager network element should try first for authentication for the domain.
20. Click **Add**.

    The information you entered appears at the top of the table.
21. Repeat Steps 19 and 20 for all other directory servers that the Collaboration Agent Manager network element can try for authentication for the domain.

    ✱ **Note:**

    The order in which the information is displayed in the table indicates the order in which the authentication servers are queried. Be sure to prioritize the list of authentication servers for each physical site based on availability or network access.
22. Repeat Steps 18 through 21 for all other Collaboration Agent Manager servers in the Avaya Aura Conferencing deployment.

**Note:**

Be sure to prioritize the list of authentication servers for each physical site based on availability or network access.

**Related links**

Integrating Avaya Aura Conferencing with LDAP directory servers on page 498

# Configuring the directory synchronization service

## Before you begin

You must have the following information:

- the Provisioning Manager you want to perform the synchronization
- the directory distinguished name from which users must be synchronized for the domain
- the directory attribute of the directory user that you want to map to the login name for Avaya Aura® Conferencing
- the directory attributes that you want to map to the Avaya Aura® Conferencing fields

## About this task

Use the following procedure to:

- configure the directory synchronization service settings
- test the connection and schema settings
- configure directory filters for a specific user domain
- perform a synchronization
- schedule a synchronization to be performed

## Procedure

1. In the Provisioning Client window, select **System Management > Directory Access Services > Synchronization Service**.
2. Click the **Sync Configuration** tab.
3. From the Select Provision manager for sync box, select the Provisioning Manager network element that you want to perform the synchronization.
4. In the Connection Timeout (milliseconds) box, enter the connection timeout in milliseconds for synchronization. If the directory synchronization client cannot establish a connection within the period you specify, the client aborts the synchronization attempt.

   **Note:**

   If you enter 0, the connection timeout is handled by TCP protocol.

5. In the Read Timeout (milliseconds) box, enter the read timeout in milliseconds for synchronization. If the directory synchronization client does not receive a read response within the period you specify, the client aborts the read attempt.

   **Note:**

   If you enter 0, there is not timeout, and the system will wait for the read operation to complete.

6. Click **Save**.
7. Click the **Sync Schema** tab.
8. From the Select domain box, select the directory domain you want to configure.
9. In the Directory distinguished name box, enter the directory distinguished name (base distinguished name or root distinguished name) from which the users must be synchronized for the domain (for example, `cn=Users,dc=ca,dc=avaya,dc=com`).
10. In the Login name box, enter the directory attribute of the directory user that you want to map to the login name for Avaya Aura Conferencing.
11. Enter all other directory attributes that you want to map to the Avaya Aura Conferencing fields displayed on this page.

    You must specify the following fields:

    - First name
    - Last name
    - Communication address handle

      The Communication address handle is a communication address without a domain. For example, if the communication address is *12345@yourcompany.com*, the handle is *12345*. If you map the email field from the directory to this field, you may receive the wrong communication address after the synchronization. For example, you may receive data with the domain repeated twice (*12345@yourcompany.com@yourcompany.com*). The domain is added automatically to the communication address handle during synchronization.

    **Note:**

    Make sure you map the following fields to unique fields in the directory:

    - Moderator access code
    - Participant access code
    - Moderator passcode
    - Participant passcode

12. When finished, click **Save**.
13. Click the **Query Test Tool** tab and test the connection and schema settings.

    Using Query Test Tool tab, you can test the connection and schema settings at any time. To test the LDAP query, you must specify an LDAP filter. For example, you may try the filter "cn=*". This filter will query all users under the base distinguished name you specified in the schema.

14. Click the **Sync Filter & Defaults** tab.

    Using the Sync Filter & Defaults tab, you can configure directory filters for a specific user domain.

    You must define one filter for each group of users you want to synchronize from the directory server. For example, if you want to synchronize users with the job title "engineer," you may define the filter "title=engineer." You can set a specific template for these users. Then, you may define a filter and default for managers. For example, this filter could be "title=manager" with a more advanced template "executive_passcodes."

    **Note:**

    Keep in mind the following:

    - Synchronization will not occur unless at least one filter is configured.
    - A filter with an empty filter value is equivalent to "query all users".

    The syntax of the filter string is defined by RFC 2254, The String Representation of LDAP Search Filters. This RFC may be used as a reference for constructing more complex filter strings.

    A filter is a UTF-8 formatted string that has the following syntax:

    (*attribute operator value*)

    or

    (*operator(filter1)(filter2)*)

    where *filter1* and *filter2* have the syntax displayed on the first line, and the operator is a string operator. The *attribute* corresponds to an LDAP attribute that exists in the directory, and value corresponds to the actual data value that is requested for the attribute. An example filter is `(&(ou=Austin)(sn=Miller))`. This filter returns all users whose last name is "Miller" and also have the organization unit "Austin."

    An attribute specified in the filter can be any attribute that exists in the LDAP directory, and it is not required to be one of the attributes (specified in translation schema) that is imported by Provisioning Manager. The attribute is used only on the LDAP server to select data, and the corresponding entries will have a subset of their data imported (based on the translation schema).

15. To configure a directory filter for a user domain, perform the following steps:

    a. From the Select domain box, select the directory domain you want to configure.

    b. In the Name box, enter the name for this filter.

    c. In the Filter box, enter the string representation of an LDAP search filter.

    d. If you want to use a specific template, select the appropriate template from the Template box.

e. If you want to use a specific location, select the appropriate location from the Location box.

f. If you want to use a specific locale, select the appropriate locale from the Local box.

g. If you want to use a specific time zone, select the appropriate time zone from the Time zone box.

h. In the Communication profile box, enter the appropriate communication profile (for example, `Primary`).

i. Click **Save**.

The new filter appears at the bottom of the table.

> **Note:**
>
> The order in which the filters are displayed in the table indicates the order in which the filters are run.

16. Repeat Step 15 if you want to create another filter.
17. Click the **Sync Scheduler** tab.
18. If you want to perform a synchronization now, click **Sync Now**.
19. If you want to schedule a synchronization for a specific time and at a specific frequency (daily, weekly, and/or monthly), perform the following steps:

a. Click the **Enable scheduled sync** check box.

b. In the Time boxes, specify the time of day you want to run the synchronization.

c. If you want to schedule the synchronization to run on specific days of the week, select **Day of Week** from the Type box, and then click the check box of the appropriate day(s).

d. If you want to schedule the synchronization to run on a specific day of the month, select **Day of Month** from the Type box, and then select the appropriate day from the Perform sync every month at the following day box.

> **Note:**
>
> If the day number you specify exceeds the last day of a month, the synchronization will run on the last day of the month. For example, if you select **31**, the synchronization will run on the last day of the month in months that have less than 31 days.

e. When finished, click **Save**.

**Related links**

Integrating Avaya Aura Conferencing with LDAP directory servers on page 498

## Configuring the directory authentication service

### About this task

Use the following procedure to configure the following settings for the directory authentication service:

- connection timeout
- read timeout

✳ **Note:**

Set these values based on the network and required user experience. Users logging into Collaboration Agent will experience the total amount of time configured here as the total amount of wait time before their login fails due to connection/read issues to the directory.

### Procedure

1. In the Provisioning Client window, select **System Management > Directory Access Services > Authentication Service**.
2. Click the **Auth Configuration** tab.
3. In the Connection Timeout (milliseconds) box, enter the connection timeout in milliseconds for authentication. If the directory authentication client cannot establish a connection within the period you specify, the client aborts the connection attempt.

   ✳ **Note:**

   If you enter 0, the connection timeout is handled by TCP protocol.
4. In the Read Timeout (milliseconds) box, enter the read timeout in milliseconds for authentication. If the directory authentication client does not receive a response within the period you specify, the client aborts the read attempt.

   ✳ **Note:**

   If you enter 0, there is no timeout, and the system will wait for the authentication operation to complete.
5. Click **Save**.

**Related links**

Integrating Avaya Aura Conferencing with LDAP directory servers on page 498

## Configuring the directory access passcode settings

### Before you begin

If you want to store encrypted passcodes on the LDAP server and in the Avaya Aura® Conferencing, see Passcodes encryption on page 512.

## About this task

Use the following procedure to configure the following directory access passcode settings for a domain:

- data source
- encoding method
- authentication key
- authentication action

**Note:**

- Changes to the encoding method and authentication key may cause encrypted passcodes stored in the external directory to become out of sync with the method Avaya Aura Conferencing will use to decrypt the passcodes. Any changes you make to these values may require you to update encrypted passcode values in the external directory and then synchronize these values to Avaya Aura® Conferencing.
- Changing the data source from the Avaya Aura Confencing database to LDAP will override passcodes with the values from the directory server during the next synchronization.

Passcode validation is enabled when the Conference Profile has passcodes enabled. Users enter the moderator or participant passcode (if required) after the participant collaboration code. The passcode is validated by either the LDAP server or the local Avaya Aura Conferencing database when the user logs into the audio/video conference or Web Collaboration Agent.

## Procedure

1. In the Provisioning Client window, select **System Management > Directory Access Services > Authentication Service**.
2. Click the **Auth Passcode** tab.
3. From the Select domain box, select the domain you want to configure.
4. From the Data Source box, select the source you want to use to validate passcodes for users when they log into an audio/video conference or Web Collaboration Agent. Your choices are **LDAP** and **AAC Database**.
5. From the Encoding Method box, select the encoding method you want to use for passcode authentication.
6. In the Authentication Key box, enter the authentication key that you want to use to decrypt passcodes.

   The authentication key uses an AES cypher with a key length of either 128 bits or 256 bits. The key should be provided in hexadecimal format. A 128 bits key will have 32 hexadecimal characters. A 256 bits key will have 64 hexadecimal characters. Passcodes are stored encrypted on the LDAP server (if the data source is LDAP). To validate the passcodes during login, the system decrypts the value from the LDAP server and compares that value with the value entered by the user during login. You may enter the value 0123456789ABCDEF0123456789ABCDEF from the example in Passcodes encryption on page 512 or your own key in the Authentication Key box. For more information, see Passcodes encryption on page 512.

7. In the Confirm Authentication Key box, re-enter the authentication key string.
8. From the Authentication Action box, select the action you want performed when LDAP is unavailable for authentication. Your choices are **Authenticate with AAC Database** and **Block Admission**.
9. Click **Save**.
10. Repeat Steps 3 through 9 for each domain.

**Related links**

Integrating Avaya Aura Conferencing with LDAP directory servers on page 498

# Passcodes encryption

For additional security, Avaya Aura® Conferencing supports encrypted passcodes stored as base64 text strings on the LDAP server and the Avaya Aura® Conferencing database.  The Advanced Encryption Standard (AES) is the only supported encryption algorithm using Cipher-block Chaining (CBC) mode with key sizes of either 128 or 256 bits. PKCS5 is used for padding.

Avaya Aura® Conferencing decrypts passcodes by first base64 decoding the passcode value. Then, it removes the first 16 bytes of the result and uses this value as the initialization vector (IV) along with the provisioned key to decrypt the remaining bytes, representing the cipher text. Passcodes are decrypted as needed. Passcodes only use the available provisioned key and cipher during the decryption process.

Avaya Aura® Conferencing will only decrypt passcodes based on the above criteria.

**Related links**

Integrating Avaya Aura Conferencing with LDAP directory servers on page 498

# Configuring multiple directory domains

## About this task

Use the following procedure to configure additional directory domains (if you added multiple directory domains).

## Procedure

1. Configure the directory servers for another directory domain you added. See Configuring directory servers on page 504.
2. Configure the directory synchronization service for the directory domain you configured in Step 1. See Configuring the directory synchronization service on page 506.

3. Configure the directory authentication service. See Configuring the directory authentication service on page 510.
4. Configure the directory access passcode settings. See Configuring the directory access passcode settings on page 510.
5. Repeat Steps 1 through 4 for the remaining directory domains you added.

**Related links**

Integrating Avaya Aura Conferencing with LDAP directory servers on page 498

## Configuring LDAP directory-synchronized users on System Manager

### About this task

Use the following procedure to provision manually on Avaya Aura® System Manager each user that you want synchronized from the LDAP directory.

### Procedure

1. Log into Avaya Aura® System Manager.
2. On the System Manager console, click **Users** > **User Management**.
3. In the navigation pane, click **User Management** > **Manage Users**.
4. On the User Management page, click **New**.

   The New User Profile page appears.
5. On the **Identity** tab, complete the required information. When entering this information, perform the following steps:
   - Make sure the data you enter in the Last Name box matches the data in the schema you mapped to “Last name” on the Sync Schema tab in Provisioning Client (Step 11 in Configuring the directory synchronization service on page 506).
   - Make sure the data you enter in the First Name box matches the data in the schema you mapped to “First name” on the Sync Schema tab in Provisioning Client (Step 11 in Configuring the directory synchronization service on page 506).
6. When finished, click **Commit & Continue**.
7. On the **Communication Profile** tab, complete the required information:

   a. **Name**: Type a name.

   b. **Default**: Select this check box.

   c. Complete the **Communication Address** section to add the user’s communication address.

**Note:**

The user's communication address consists of a handle and a domain (for example, 5522@avaya.com). When entering this information:

- Make sure the data you enter for the handle matches the data in the schema you mapped to "Communication address handle" on the **Sync Schema** tab in Provisioning Client (Step 11 in Configuring the directory synchronization service on page 506).
- Make sure the data you enter for the domain matches the domain you selected on the **Sync Schema** tab in Provisioning Client (Step 8 in Configuring the directory synchronization service on page 506).

d. Complete the **Session Manager Profile** section.

e. Complete the following profiles as required for your users:

- **CallPilot Messaging Profile**
- **CM Endpoint Profile**
- **CS 1000 Endpoint Profile**
- **Messaging Profile**
- **B5800 Branch Gateway Endpoint profile**

**Note:**

Do not assign the Conferencing Profile to the user. The user will be synchronized into Avaya Aura Conferencing. If you assign the Conferencing Profile, you will receive errors either when saving the user on System Manager or during a subsequent LDAP synchronization because two sources will be trying to modify the same user data in Avaya Aura Conferencing.

8. Click **Commit & Continue**.
9. Repeat Steps 4 through 8 for each new user you want to add to System Manager.

**Related links**

Integrating Avaya Aura Conferencing with LDAP directory servers on page 498

# Retrieving the CA certificate from the Active Directory server

## About this task

Use the following procedure to retrieve the CA certificate from the Active Directory server.

**Note:**

Perform this procedure only if you are using TLS to connect to the Active Directory server.

## Procedure

1. Log into the Active Directory server as administratior.
2. Open the Certificates console:
    a. Click **Start**.
    b. Type `MMC` and press the ENTER key.
    c. If prompted by the User Account Control, make sure the action you want to perform is displayed, and click **Yes**.
3. In the MMC console window, click **File**, and then click **Add/Remove Snap-in**.
4. In Add or Remove Snap-ins under Available Snap-ins, click **Certificates**, and then click **Add**.
5. In Certificates snap-in, select **Computer account**, and then click **Next**.
6. Perform one of the following steps:
    - If you are managing the LDAP server requiring the certificate, select **Local**.
    - If you are not managing the LDAP server requiring the certificate, select **Another computer**, click **Browse**, and select the LDAP server requiring the certificate.
7. Click **OK**.
8. Click **Finish**.
9. In Add or Remove Snap-ins, click **OK**.
10. In the console tree, expand Certificates (<computer>).
11. Go to **Personal**.
12. Go to **Certificates**.
13. Select a topmost certificate.
14. Right-click the certificate, and select **All Tasks > Export**.
15. In the Export dialog box:
    - Do not export private key.
    - Select **User base64 encoding format**.
16. Save to a file. Use a filename similar to ADserver_CA_base64.cer.

**Related links**

Integrating Avaya Aura Conferencing with LDAP directory servers on page 498

# Assigning the Directory Server Certificate for the network elements

### About this task

Use this procedure to set the certificate/key from the keystore for any directory servers configured for mutual/client authentication to Directory Server Certificate for the following network elements:

- Application Server
- Provisioning Manager
- Collaboration Agent Manager

### Procedure

1. In the navigation pane of Element Manager Console, click **Feature Server Elements > Provisioning Managers**.
2. In the Provisioning Managers window, select the first Provisioning Manager ( for example, **PROV1**).
3. Click **Edit (-/+)**.
4. From the Directory Server Certificate box in the Edit dialog box, select the appropriate certificate.
5. Click **Apply**.
6. Repeat Steps 2 through 5 for any additional Provisioning Managers.
7. In the navigation pane of Element Manager Console, click **Feature Server Elements > Application Servers**.
8. In the Application Servers window, select the first Application Server (for example, **AS1**).
9. Click **Edit (-/+)**.
10. From the Directory Server Certificate box in the Edit dialog box, select the appropriate certificate.
11. Click **Apply**.
12. Repeat Steps 8 through 11 for any additional Application Servers.
13. In the navigation pane of Element Manager Console, click **Feature Server Elements > Collaboration Agent Managers**.
14. In the Collaboration Agent Managers window, select the first Collaboration Agent Manager (for example, **CA1**).
15. Click **Edit (-/+)**.
16. From the Directory Server Certificate box in the Edit dialog box, select the appropriate certificate.
17. Click **Apply**.

18. Repeat Steps 14 through 17 for any additional Collaboration Agent Managers.

**Related links**

Integrating Avaya Aura Conferencing with LDAP directory servers on page 498

# Chapter 31: Deploying integrated audio and video

## Deploying integrated audio and video

In the context of Avaya Aura® Conferencing, “integrated audio and video” means that users can receive their audio and their video feeds through the Web. This functionality means that users do not have to dial into the conference using a phone connection. The Collaboration Agent user application provides users with all they need to interact with other participants.

In this release, Avaya provides two types of integrated audio and video. They are called:

- Audio/Video in Collaboration Agent
- Avaya Web Collaboration audio and video plug-in

### Audio/Video in Collaboration Agent

This form of integrated audio and video is delivered using a Flash-based client. To enable this form of integrated audio and video, you must install and configure a Flash Media Gateway (FMG). Avaya Aura® Conferencing requires Adobe Flash 11.2 or later. Avaya introduced this client in release 7.2 of Avaya Aura® Conferencing. If you have an existing installation of Avaya Aura® Conferencing 7.x, you can continue to use this client. However, Avaya recommends upgrading to the new method of integrated audio and video, which is delivered as a browser plug-in.

### Avaya Web Collaboration audio and video plug-in

This form of integrated audio and video is delivered using a browser plug-in. This form of integrated audio and video offers an improved audio and video experience and a more intuitive user interface. If you wish to offer this form of integrated audio and video to external users who reside outside of the enterprise, you must install and configure a Session Border Controller (SBC).

**Related links**

Audio/Video in Collaboration Agent on page 518

Avaya Web Collaboration audio and video plug-in on page 549

## Audio/Video in Collaboration Agent

Audio/Video in Collaboration Agent is a Flash-based client. Avaya introduced this client in release 7.2 of Avaya Aura® Conferencing. If you have an existing installation of Avaya Aura® Conferencing

7.x, you can continue to use this client. However, Avaya recommends upgrading to the new method of integrated audio and video, which is delivered as a browser plug-in.

**Related links**

Pre-deployment checklist for Audio/Video in Collaboration Agent on page 519
Checklist for installing Audio/Video in Collaboration Agent on page 522
Configuring ports for Audio/Video in Collaboration Agent on page 525
Accessing and extracting the Audio/Video in Collaboration Agent installation files on page 527
Configuring Audio/Video in Collaboration Agent for an SMB or medium deployment on page 528
Installing the Audio/Video in Collaboration Agent server software on page 529
Installing the Audio/Video in Collaboration Agent Management Portal software on page 532
Configuring the Flash Media Gateway on page 533
Adding a Flash Media Gateway cluster on page 535
Starting the Flash Media Gateway on page 537
Creating the client configuration file on page 538
Installing the Audio/Video in Collaboration Agent client software on page 539
Enabling Audio/Video in Collaboration Agent in the Provisioning Manager on page 540
Verifying integration of the multimedia client software with Collaboration Agent on page 541
Hardening Audio/Video in Collaboration Agent on page 542
Upgrading Audio/Video in Collaboration Agent on page 549
Deploying integrated audio and video on page 518
Avaya Web Collaboration audio and video plug-in on page 549

## Pre-deployment checklist for Audio/Video in Collaboration Agent

The following checklist provides the high level steps and considerations prior to beginning your installation of Audio/Video in Collaboration Agent.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Ensure that Avaya Aura® Conferencing is installed and operating properly prior to installing Audio/Video in Collaboration Agent. | | | |
| 2 | Obtain the following information for the Avaya Aura® Conferencing system:<br>• IP address of each Provisioning Manager | | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| | that will host the Management Portal Client and its supporting files<br>• IP address of each Collaboration Agent Manager that will host the Audio/Video in Collaboration Agent client and its supporting files<br>• Avaya Aura® Conferencing service domain<br>• Avaya Aura® Conferencing MeetMe Conference service name<br>• Avaya Aura® Conferencing Event Conference service name | | | |
| 3 | If you plan to control access to Audio/Feature in Collaboration Agent, determine the service network topology (as IP address ranges). Provisioning Manager will control access to this feature by IP address range. | | | |
| 4 | Obtain the IP address of the System Manager that will be used to establish a SIP trunk for each Flash Media Gateway, and add a SIP entity for each Flash Media Gateway in the System Manager. | In the case of a Turnkey solution, you require the equivalent values for your PBX. | | |
| 5 | Determine the dedicated IP address and FQDN for each server that will | | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| | host a Flash Media Gateway instance.<br>For systems with more than one Flash Media Gateway, identify which Flash Media Gateway instance will also host the simplex Management Server.<br>For systems with more than two Flash Media Gateways, identify which Flash Media Gateway instances will perform the Load Balancer function. You can have a maximum of two Flash Media Gateways performing the Load Balancer function. | | | |
| 6 | If secure communication links are required, obtain security certificates from a public Certificate Authority. | | | |
| 7 | Identify the target server that will host the Audio/Video Management Server for the system. | | | |
| 8 | Ensure that the enterprise firewall is configured to support delivery of Audio/Video in Collaboration Agent capabilities.<br>If you are using a DMZ deployment, consider the following:<br>• Ensure you have configured the required servers, routers, and firewalls. | Contact your network specialist or administrator if you have a large deployment and require a DMZ configuration.<br>For more information, see Enterprise DMZ deployment on page 45. For the complete *Port Matrix: Avaya Aura® Conferencing* document, go to http://support.avaya.com. | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| | - Ensure the required port modifications are made. | | | |
| 9 | Make sure the server on which you will install Audio/Video in Collaboration Agent is supported. | | | |
| 10 | Obtain the Avaya Aura® Conferencing disks for Linux and software installation, and patches:<br>- AAC platform DVD-ROM<br>- Application Bundle DVD-ROM<br>- Platform patches DVD-ROM<br>To install Audio/Video for Collaboration Agent, you must have the following software:<br>- AccWeb-a-b-c.i386.rpm.bin (This is the server software.)<br>- AccWeb-clients-d-e.zip (This is the Management Portal software.)<br>- AacpaOtv-client-f-g.zip (This is the client software that will be integrated with Collaboration Agent.) | | | |

**Related links**

Audio/Video in Collaboration Agent on page 518

## Checklist for installing Audio/Video in Collaboration Agent

The following checklist provides a high-level view of the tasks involved in installing Audio/Video in Collaboration Agent.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Download the latest edition of the *Avaya Aura*® *Conferencing Intelligent Workbook*, which is available from https://support.avaya.com/. | This Microsoft Excel file contains all the configuration information required to configure Audio/Video in Collaboration Agent. It is divided into a series of worksheets. | | |
| 2 | Ensure you have gathered the information required to install Audio/Video in Collaboration Agent. | See Pre-deployment checklist for Audio/Video in Collaboration Agent on page 519. | | |
| 3 | Open the appropriate ports between the Internet, DMZ, and enterprise networks. | See Configuring ports for Audio/Video in Collaboration Agent on page 525. | | |
| 4 | Install the hardware (if required). | See Installing the server in the rack on page 93 | | |
| 5 | Configure RAID arrays. | See Managing Hewlett Packard Smart Arrays on page 97 | | |
| 6 | If you are using a standalone server for the Flash Media Gateway, perform the following steps:<br>1. Install the Linux operating system on that server.<br>**Important:**<br>The “Installing the AAC Platform” procedure guides you through the installation process with links to individual procedures. Upon completion of each step, return to the next step in the “Installing the AAC Platform” procedure by clicking the link at the end of each individual procedure. | See:<br>• Installing the AAC Platform on page 121 | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| | 2. Verify that all the required components are operational and error free after completing the Linux operating system installation. | | | |
| 7 | Extract the Audio/Video in Collaboration Agent software loads from the AAC Application Bundle iso image. | See Accessing and extracting the Audio/ Video in Collaboration Agent installation files on page 527. | | |
| 8 | If you are installing Audio/ Video in Collaboration Agent in an SMB or medium deployment with other Avaya Aura® Conferencing components, you must add the IP address of the co-resident Flash Media Gateway using the **`mcpModIPv4Subnet`** command. | See Configuring Audio/ Video in Collaboration Agent for an SMB or medium deployment on page 528. | | |
| 9 | Install the Flash Media Gateway server software. | See Installing the Audio/ Video in Collaboration Agent server software on page 529. | | |
| 10 | Install the Management Portal Client software. | See Installing the Audio/ Video in Collaboration Agent Management Portal software on page 532. | In particular, ensure that you install the required certificate, as described in this task. | |
| 11 | Configure the Flash Media Gateway. | See Configuring the Flash Media Gateway on page 533. | | |
| 12 | Add a Flash Media Gateway cluster. | See Adding a Flash Media Gateway cluster on page 535. | | |
| 13 | Place the Flash Media Gateway in service. | See Starting the Flash Media Gateway on page 537. | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 14 | Create the configuration file for the Audio/Video in Collaboration Agent client. | See Creating the client configuration file on page 538. | | |
| 15 | Install the Audio/Video in Collaboration Agent client software. | See Installing the Audio/Video in Collaboration Agent client software on page 539. | | |
| 16 | Enable Audio/Video in Collaboration Agent. | See Enabling Audio/Video in Collaboration Agent in the Provisioning Manager on page 540. | | |
| 17 | Verify that the Audio/Video in Collaboration Agent client software is integrated properly with Collaboration Agent. | See Verifying integration of the multimedia client software with Collaboration Agent on page 541. | | |
| 18 | Secure Audio/Video in Collaboration Agent. | See Hardening Audio/Video in Collaboration Agent on page 542. | | |

**Related links**

Audio/Video in Collaboration Agent on page 518

## Configuring ports for Audio/Video in Collaboration Agent

### About this task

Use this procedure to configure the ports for Audio/Video in Collaboration Agent.

### Procedure

1. Configure the ports between the Internet and the DMZ. See the following table:

**Table 27: Ports between the Internet and the DMZ**

| Server | Port Name | Description |
|---|---|---|
| Collaboration Agent Manager | Port 443 for HTTPS | This port leads to a secure web page for the user. |
| Flash Media Gateway<br>**Note:**<br>RTMPT provides the highest level of usability. However, | Port 80 | This port is for RTMPT, which is a tunneled version of the RTMP protocol for the Audio/Video for Collaboration Agent flash client. |

*Table continues…*

| Server | Port Name | Description |
|---|---|---|
| the most secure method is RTMPS. Avaya recommends the use of the RTMPS protocol, except in cases where RTMPS is blocked by personal computer or corporate firewalls. In these cases, the use of RTMPT usually resolves any blockage. | Port 1935 | This port is for RTMP for the user flash client. |
| | Port 443 | This port is for RTMPS, which is a secure SSL version of the RTMP protocol for the user flash client. |

2. Configure the ports used inside the DMZ. See the following table:

**Table 28: Ports between the Internet and the DMZ**

| Server | Port Name | Description |
|---|---|---|
| Flash Media Gateway | Port 9444 | This port is for the JMX-RMI connection from the Management Server to the Flash Media Gateway. |
| | Port 9445 | This port is for the JMX-RMI connection from the Flash Media Gateway to the Load Balancer server. |
| | Ports 5080 and 9999 | These ports are internal to the Flash Media Gateway server. |

3. Configure the ports between the DMZ and the enterprise.

**Table 29: Ports between the Internet and the DMZ**

| Server | Port Name | Description |
|---|---|---|
| Collaboration Agent Manager | Port 443 for HTTPS | This port leads to a secure web page for the user. This port should be allowed if:<br>• Audio/Video for Collaboration Agent access is required inside the enterprise<br>• Collaboration Agent has the Audio/Video for Collaboration Agent client deployed and is located in the DMZ |
| Flash Media Gateway | Port 5060 | This port is the SIP TCP connection to the SIP proxy (for example, to the Session Border Control application). |

*Table continues…*

| Server | Port Name | Description |
|---|---|---|
| | Port 5061 | This port is the SIP TLS connection to the SIP proxy (for example, to the Session Border Control application). |
| | RTP Port range | This is the range of ports used for RTP as configured on the Flash Media Gateway. Two ports are required for each audio session, and four ports are required for each audio/video session.<br>**Note:**<br>The RTP connection is required only between the Flash Media Gateway and the hosting Avaya Media Servers. |
| | Ports 80, 1935, and 443 | These ports are for RTMPT (port 80), RTMP (port 1935), RTMPS (port 443) if:<br>• Audio/Video in Collaboration Agent access is required inside the enterprise<br>• the Flash Media Gateway that provides Audio/Video in Collaboration Agent is deployed in the DMZ |
| | Port 9443 | This port is for RTMPS for the Flash Media Gateway Management Portal. This port is required if the Management Server is deployed inside the DMZ, which is not recommended. |

**Related links**

Audio/Video in Collaboration Agent on page 518

## Accessing and extracting the Audio/Video in Collaboration Agent installation files

### Before you begin

Make sure you have the latest version of the Avaya Aura® Conferencing Application Bundle. You can download iso images of this software from PDLS and burn the iso images to DVD-ROM.

### About this task

Use this procedure to copy the Avaya Aura® Conferencing Application Bundle iso image to the primary Element Manager server and extract the Audio/Video in Collaboration Agent software. The Audio/Video in Collaboration Agent software consists of the following components:

- AccWeb-a-b-c.i386.rpm.bin

  This is the Flash Media Gateway server software.

- AccWeb-clients-d-e.zip

  This is the Management Portal Client software.
- AacpaOtv-client-f-g.zip

  This is the Audio/Video in Collaboration Agent (AViCA) client software.

### Procedure

1. Log on to the primary Element Manager server as a user with the SA role (for example, `ntappadm`) through ssh or directly at the server console.
2. Copy the Avaya Aura® Conferencing Application Bundle iso file to the directory `/var/mcp/extract`on the primary Element Manager server.
3. Access the directory `/var/mcp/extract`.
4. Use the command `mcpExtractContent` to extract the content.

   The software is extracted to the directory `/var/mcp/media/avica`. This directory should contain the following files:

   - AccWeb-a-b-c.i386.rpm.bin
   - AccWeb-clients-d-e.zip
   - AacpaOtv-client-f-g.zip

### Next steps

Proceed to Installing the Audio/Video in Collaboration Agent server software on page 529.

#### Related links

Audio/Video in Collaboration Agent on page 518

## Configuring Audio/Video in Collaboration Agent for an SMB or medium deployment

In previous releases, SMB and medium deployments were known as 'co-resident' deployments. In these deployments, several conferencing elements reside on a single server.

### Before you begin

You must know the IP address of the co-resident Flash Media Gateway. This is equivalent to the network element instance service address.

### About this task

Use this procedure to configure Audio/Video in Collaboration Agent for an SMB or medium deployment.

### Procedure

1. Using Element Manager Console, stop all network element instances deployed on the selected server. For more information, see Stopping and undeploying a network element instance on page 628.

2. Log on to the target server as `ntsysadm` through ssh or directly on the server console.
3. At the prompt, type `mcpModIPv4Subnet -name sn0 -addotheraddrs <FMG.CO.RES.IP>` where *<FMG.CO.RES.IP>* is the network element instance service address.
4. Press **Enter**.
5. Using Element Manager Console, start all the network element instances deployed on the selected server. For more information, see Starting a network element instance on page 669.

**Related links**

Audio/Video in Collaboration Agent on page 518

## Installing the Audio/Video in Collaboration Agent server software

### Before you begin

You must be able to access the Audio/Video in Collaboration Agent server software (AccWeb-a-b-c.i386.rpm.bin).

### About this task

Use this procedure to install the Audio/Video in Collaboration Agent server software. You will install this software on the Flash Media Gateway server.

### Procedure

1. Log on to the Flash Media Gateway server as `ntsysadm` through ssh or directly on the server console.
2. Enter **`su -`** to log on as root.
3. At the prompt `password`, type the root password, and press **Enter**.
4. Make sure the directory `/var/mcp/media/avica` exists on the Flash Media Gateway server.

   If this directory does not exist, perform the following steps to create the directory:

   a. At the prompt, type `mkdir -m 770 /var/mcp/media/avica` and press **Enter**.
   b. At the prompt, type `chown -R ntappsw:ntappgrp /var/mcp/media/avica` and press **Enter**.
5. Copy the file `AccWeb-x-x-x.i386.rpm.bin` from the directory `/var/mcp/media/avica` on the primary Element Manager server into the directory `/var/mcp/media/avica` on the Flash Media Gateway server.
6. Go to the directory `/var/mcp/media/avica` on the Flash Media Gateway server.
7. Type `chmod +x AccWeb-x.x-x.i386.rpm.bin` and press **Enter**.
8. Type `./AccWeb-x.x-x.i386.rpm.bin` and press **Enter**.

The Avaya Customer Connections Web End User License Agreement (EULA) appears.

9. Read the license agreement.
10. To accept the license agreement and proceed with the installation, type `y` .

    The software is installed on the server. During the installation, the FMG software is installed in the directory `/var/mcp/rum/fmg`, and Red5 Media Server is installed in the directory `/var/mcp/run/red5`.

    You are prompted to run the configuration tool.

    **Note:**

    In this procedure, you will run the configuration tool now. However, you can manually run the configuration tool at a later time by accessing `/var/mcp/run/fmg/bin` and then using the command **`/var/mcp/rum/fmg/bin`**.

    **Warning:**

    At each step, the configuration tool provides a default option. Ensure that you check each default option because it may not be the correct IP address. Do not simply accept each default value.
11. Type `y`, and press **Enter**.

    You are prompted to enter the IP address for the JMX connections.
12. Perform one of the following steps:
    - If you want to use the default, press **Enter**.
    - If you want to use a different IP address, enter the appropriate IP address, and then press **Enter**.
13. When prompted to enter the IP address for the RTMP connections, perform one of the following steps:
    - If you want to use the default, press **Enter**.
    - If you want to use a different IP address, enter the appropriate IP address, and then press **Enter**.
14. When prompted to enter the IP address for the HTTP connections, perform one of the following steps:
    - If you want to use the default, press **Enter**.
    - If you want to use a different IP address, enter the appropriate IP address, and then press **Enter**.
15. When prompted to enable RTMPS, type `y`, and press **Enter**.
16. When prompted to enter the port for RTMPS, perform one of the following steps:
    - If you want to use the default, press **Enter**.
    - If you want to use a different port, enter the appropriate port, and then press **Enter**.

17. When prompted to generate a self-signed certificate for RTMPS, type `y`, and press **Enter**.
18. When prompted to enable RTMP, type `y`, and press **Enter**.
19. When prompted to enter the port for RTMP, perform one of the following steps:
    - If you want to use the default, press **Enter**.
    - If you want to use a different port, enter the appropriate port, and then press **Enter**.
20. When prompted to enable RTMPT, type `y`, and press **Enter**.
21. When prompted to enter the port for RTMPT, perform one of the following steps:
    - If you want to use the default, press **Enter**.
    - If you want to use a different port, enter the appropriate port, and then press **Enter**.

    You are prompted to enter the IP address for the Management Client.
22. Perform one of the following steps:
    - If you want to use the default, press **Enter**.
    - If you want to use a different IP address, enter the appropriate IP address, and then press **Enter**.
23. When prompted to enter the port for the Management Client, press **Enter**.

    You are prompted to run the Management Server on this machine.
24. Perform one of the following steps:
    - If this machine is the primary Flash Media Gateway in the cluster or this machine is a standalone Flash Media Gateway Management server co-located with Provisioning Manager if all Flash Media Gateways are in the DMZ, type `y`, and press **Enter**.
    - If this machine is *not* the primary Flash Media Gateway in the cluster or this machine is *not* a standalone Flash Media Gateway Management server co-located with Provisioning Manager if all Flash Media Gateways are in the DMZ, type `n`, and press **Enter**.
25. When prompted to generate a self-signed certificate for RTMPS for the Management Portal, type `y`, and press **Enter**.
26. At the command prompt, type `source /root/.bash_profile` and press **Enter** to apply the environment variables that were added during installation.
27. At the command prompt, type `service red5 start` and press **Enter** to start the server as a Linux service.

## Next steps

Proceed to Installing the Audio/Video in Collaboration Agent Management Portal software on page 532.

### Related links

Audio/Video in Collaboration Agent on page 518

# Installing the Audio/Video in Collaboration Agent Management Portal software

### Before you begin

You must be able to access the Audio/Video in Collaboration Agent Management Portal software (AccWeb-clients-d-e.zip).

### About this task

Use this procedure to install the Audio/Video in Collaboration Agent server software. You will install this software on the Element Manager server where the Provisioning Manager (PROV) is installed.

### Procedure

1. Log on to the Element Manager server where the Provisioning Manager is installed as `ntsysadm` through ssh or directly on the server console.
2. Enter **`su -`** to log on as root.
3. At the prompt `password`, type the root password, and press **Enter**.
4. Make sure the directory `/var/mcp/media/prov_pa_installs` exists on the target server.

   If this directory does not exist, perform the following steps to create the directory:

   a. At the prompt, type `mkdir -m 770 /var/mcp/media/prov_pa_installs` and press **Enter**.

   b. At the prompt, type `chown -R ntappsw:ntappgrp /var/mcp/media/prov_pa_installs` and press **Enter**.
5. Make sure the directory `/var/mcp/media/prov_pa_installs/fmgadmin` exists on the target server.

   If this directory does not exist, perform the following steps to create the directory:

   a. At the prompt, type `mkdir -m 770 /var/mcp/media/prov_pa_installs/fmgadmin` and press **Enter**.

   b. At the prompt, type `chown -R ntappsw:ntappgrp /var/mcp/media/prov_pa_installs/fmgadmin` and press **Enter**.
6. Copy the file `AccWeb-clients-d-e.zip` from the directory `/var/mcp/media/avica` on the primary Element Manager server into the directory `/var/mcp/media/avica` on the target server.
7. Go to the directory `/var/mcp/media/avica` on the target server.
8. At the prompt, type `unzip AccWeb-clients-d-e.zip admin/* -d fmgtemp/` and press **Enter**.

9. At the prompt, type `cp -R fmgtemp/admin/* /var/mcp/media/prov_pa_installs/fmgadmin/` and press **Enter**.
10. At the prompt, type `chown -R ntappsw:ntappgrp /var/mcp/media/prov_pa_installs/fmgadmin` and press **Enter**.
11. At the prompt, type `chmod -R 770 /var/mcp/media/prov_pa_installs/fmgadmin` and press **Enter**.
12. At the prompt, type `rm -rf fmgtemp` and press **Enter**.

### Next steps

Proceed to Configuring the Flash Media Gateway on page 533.

### Related links

Audio/Video in Collaboration Agent on page 518

## Configuring the Flash Media Gateway

### Before you begin

You must be able to access the Audio/Video in Collaboration Agent Management Portal client.

### About this task

Use this procedure to configure the Flash Media Gateway.

**Note:**

Avaya Aura Conferencing supports a maximum of four Flash Media Gateways.

### Procedure

1. Open a web browser and go to `https://<PROV IP address or FQDN>:8443/fmgadmin/index.html` where <PROV IP address or FQDN> is the IP address or FQDN of the server running Provisioning Manager.

   The Log On page for Avaya One Touch Video 3.0 appears. You will use Avaya One Touch Video 3.0 to administer the Audio/Video in Collaboration Agent feature.
2. In the User Name box, enter `admin`.
3. In the Password box, enter `admin01`.
4. Click **Log on**.

   The Security Alert dialog box appears.

   **Note:**

   The first time you access the Management Portal Client you must set up the certificate in your Truststore.
5. Click **View Certificate**.

6. In the Certificate dialog box, click **Install Certificate**.
7. In the Certificate Import Wizard dialog box, click **Next**.
8. On the Certificate Store page, select **Place all certificates in the following store**, and then click **Browse**.
9. In the Select Certificate Store dialog box, select **Trusted Root Certification Authorities**, and click **OK**.
10. On the Certificate Store page, click **Next**.
11. On the Completing the Certificate Import Wizard page, click **Finish**.
12. In the Security Warning dialog box, click **Yes**.

    The Certificate Import Wizard message box appears, indicating that the certificate import was successful.
13. In the Certificate Import Wizard message box, click **OK**.

    **Note:**

    Your initial attempt to access the Management Portal Client will fail. After the certificate is installed, you must refresh your browser window and then try to log in again.
14. Click **Log on**.

    The Legal Notice page appears.
15. On the Legal Notice page, read the information provided.
16. To accept the information displayed, click **Accept**.

    The Welcome page appears.
17. On the Welcome page, click **Add New Flash Media Gateway**.
18. In the Name box on the Flash Media Gateway page, enter a name for this Flash Media Gateway.
19. In the Management IP Address box, enter the IP address of this Flash Media Gateway that will connect to the Flash Media Gateway Management Server as specified during installation.
20. In the Management Port box, use the default setting (9444).
21. In the Externally accessible RTMP IP Address box, enter the IP address of this Flash Media Gateway that will service the Flash domain.
22. In the Server ID box, click **Get Next** to assign a unique ID to this Flash Media Gateway.
23. In the IP Address box in the SIP Trunk area, enter the IP address of this Flash Media Gateway that will establish a SIP trunk to the Avaya Aura Session Manager server as specified during installation.
24. In the Port box, use the default setting (5060).
25. Click the **Use Cluster Settings** check box to enable it.

26. In the RTP area at the bottom of the page, click **New**.
27. In the IP Address box in the RTP Bind Interfaces Table Input dialog box, enter the IP address of this Flash Media Gateway that will establish RTP/RTCP connections to the Avaya Media Server as specified during installation.
28. In the Start Port box, enter 40000.
29. In the End Port box, enter 60000.

    ✱ **Note:**

    These Start Port and End Port settings will provide a range of 10000 RTP ports and 10000 RTCP ports.
30. Click **OK**.
31. Click **Save** at the bottom of the page.
32. If you want to configure another Flash Media Gateway, repeat Steps 7 through 21.

    ✱ **Note:**

    Avaya Aura Conferencing supports a maximum of four Flash Media Gateways.

### Next steps

Proceed to Adding a Flash Media Gateway cluster on page 535.

**Related links**

Audio/Video in Collaboration Agent on page 518

## Adding a Flash Media Gateway cluster

### Before you begin

You must be able to log into the Audio/Video in Collaboration Agent Management Portal client.

### About this task

Use this procedure to add a Flash Media Gateway cluster.

✱ **Note:**

Avaya Aura® Conferencing supports one Flash Media Gateway cluster.

### Procedure

1. From the Clusters area in the navigation panel of the Avaya One Touch Video 3.0 application, click **Add New**.
2. In the Name box on the Clusters page, enter a name for this cluster.
3. In the Flash Media Gateways area, click **Add**.
4. From the Name box in the Cluster FMG Table Input dialog box, select the Flash Media Gateway you added.

5. In the Call Capacity box, enter a number that is less than or equal to the licensed capacity of the Flash Media Gateway you selected in Step 4.
6. Click **OK**.
7. In the Load Balancer area, click **Add**.
8. From the FMG Name box in the Cluster Load Balancer Table Input dialog box, select the Flash Media Gateway that will provide the Load Balancer function.
9. In the JMX Bind Interface box, enter the IP address of the Flash Media Gateway you specified in Step 8.
10. In the JMX Bind Port box, enter the appropriate port number. The default is 9445.
11. Click **OK**.
12. In the RTMPS Cipher Settings area, select **SSL_RSA_WITH_3DES_EDE_CBC_SHA** in the Available Ciphers list box.
13. Click **>>**.

    The selected cipher appears in the Selected Ciphers list box.
14. In the SIP Trunk area, enter the IP address of the Avaya Aura® Session Manager (or, if this is a Turnkey solution, enter your PBX equivalent) in the IP Address box.
15. In the Port box, enter 5060 (the default).
16. In the Agent Call Setting area, enter the service domain for Avaya Aura® Conferencing in the SIP domain box.
17. In the Customer Call Settings area, enter the service domain for Avaya Aura® Conferencing in the (From) SIP Domain box.
18. In the (To) SIP Domain box, enter the service domain for Avaya Aura® Conferencing.
19. In the Routing area, click **New**.
20. In the Route Name box in the Cluster Routing Table Input dialog box, enter the name for the route that will be used for connecting to MeetMe conferencing.
21. In the SIP User Name box, enter the service name for MeetMe conferencing.
22. In the SIP Domain box, enter the service domain for Avaya Aura® Conferencing.
23. Click **OK**.
24. In the Routing area, click **New**.
25. In the Route Name box in the Cluster Routing Table Input dialog box, enter the name for the route that will be used for connecting to Event conferencing.
26. In the SIP User Name box, enter the service name for Event conferencing.
27. In the SIP Domain box, enter the service domain for Avaya Aura® Conferencing.
28. Click **OK**.
29. In the Codecs area, select the appropriate audio codec from the Audio Codecs box.

30. From the Customer Call Audio Codecs box, select the appropriate audio codec.
31. From the Cluster Video Codecs box, select **H264**.
32. In the Profiles area, click **Add Profile**.
33. In the Enter a profile Name dialog box, enter a name for this profile, and click **OK**.
34. Click **Add**.
35. From the Video FPS box, in the Bandwidth Level Table dialog box, select **30**.
36. From the Video Size box, select **AAC_640_360**.
37. From the Video B/W box, select **512**.
38. From the AS B/W box, enter `0`. AS/BW is not supported for Avaya Aura® Conferencing.
39. From the AS Mode box, select **RESERVED**. AS Mode is not supported for Avaya Aura® Conferencing.
40. Click **OK**.
41. Click **Save** at the bottom of the page.

### Next steps

Proceed to Starting the Flash Media Gateway on page 537.

**Related links**

Audio/Video in Collaboration Agent on page 518

## Starting the Flash Media Gateway

### Before you begin

You must be able to log into the Audio/Video in Collaboration Agent Management Portal software.

### About this task

Use this procedure to place the Flash Media Gateway into service.

### Procedure

1. From the Flash Media Gateway area in the navigation panel of the Avaya One Touch Video 3.0 application, click **List All**.
2. In the System Status area of the Flash Media Gateway page, select the Flash Media Gateway.
3. Click **Start** to place the selected Flash Media Gateway into service.
4. Repeat Steps 2 and 3 for each Flash Media Gateway.

### Next steps

Proceed to Creating the client configuration file on page 538.

**Related links**

Audio/Video in Collaboration Agent on page 518

## Creating the client configuration file

### Before you begin

- All of the Flash Media Gateway are licensed and started (in service).
- You are able to log into the Audio/Video in Collaboration Agent Management Portal client.

### About this task

Use this procedure to create the configuration file for the Audio/Video in Collaboration Agent client.

### Procedure

1. From the Settings area in the navigation panel of the Avaya One Touch Video 3.0 application, click **Customer Configuration**.

   The ACC Web Customer Configuration page appears.
2. From the Cluster box, select the cluster that you created. This is the primary address that the Audio/Video in Collaboration Agent client will use to connect to the Flash Media Gateways.
3. From the Protocol box, select the protocol that the Audio/Video in Collaboration Agent client will use to establish connections across the Flash domain.
4. From the Profile Name box, select the profile that you created.
5. From the Meetme Route Name box, select the MeetMe conferencing route that you created. This is the route that the Audio/Video in Collaboration Agent client will use to connect callers to a MeetMe conference.
6. From the Event Route Name box, select the Event conferencing route that you created. This is the route that the Audio/Video in Collaboration Agent client will use to connect callers to an Event conference.
7. Check the **Audio Available** check box if you want to make the audio capability available to the Audio/Video in Collaboration Agent client using this configuration. This option is available only if licensed.
8. Check the **Video Available** check box if you want to make the video capability available to the Audio/Video in Collaboration Agent client using this configuration. This option is available only if licensed.
9. Check the Default Audio Selected check box if you want to make the audio capability available by default to the Audio/Video in Collaboration Agent client using this configuration.

10. Check the Default Video Selected check box if you want to make the video capability available by default to the Audio/Video in Collaboration Agent client using this configuration.
11. Click **Generate** to create the client configuration file (`AccWebCustomerConfig.xml`).

    The Configuration Text dialog box appears and displays the contents of the `AccWebCustomerConfig.xml`.
12. Click **Save**.
13. Using the Select location for download by dialog box, specify where you want to save the file `AccWebCustomerConfig.xml`, and then click **Save**.
14. Click **Log Off** at the top of the page to log off Avaya One Touch Video 3.0.

### Next steps

Proceed to Installing the Audio/Video in Collaboration Agent client software on page 539.

**Related links**

Audio/Video in Collaboration Agent on page 518

## Installing the Audio/Video in Collaboration Agent client software

### Before you begin

- You must be able to access the Audio/Video in Collaboration Agent client software (`AacpaOtv-client-f-g.zip`).
- You must be able to access the client configuration file you created (`AccWebCustomerConfig.xml`).

### About this task

Use this procedure to install the Audio/Video in Collaboration Agent client software and configuration file you created. You will install this software and configuration file on the Collaboration Agent Manager server.

### Procedure

1. Log on to the Collaboration Agent Manager server as `ntsysadm` through ssh or directly on the server console.
2. Enter **`su -`** to log on as root.
3. At the prompt `password`, type the root password, and press **Enter**.
4. Make sure the directory `/var/mcp/media/prov_pa_installs` exists on the target server.

    If this directory does not exist, perform the following steps to create the directory:

    a. At the prompt, type `mkdir -m 770 /var/mcp/media/prov_pa_installs` and press **Enter**.

   b. At the prompt, type `chown -R ntappsw:ntappgrp /var/mcp/media/prov_pa_installs` and press **Enter**.

5. Make sure the directory `/var/mcp/media/prov_pa_installs/otv` exists on the target server.

   If this directory does not exist, perform the following steps to create the directory:

   a. At the prompt, type `mkdir -m 770 /var/mcp/media/prov_pa_installs/otv` and press **Enter**.

   b. At the prompt, type `chown -R ntappsw:ntappgrp /var/mcp/media/prov_pa_installs/otv` and press **Enter**.

6. Copy the file `AacpaOtv-client-f-g.zip` from the directory `/var/mcp/media/avica` on the primary Element Manager server into the directory `/var/mcp/media/avica` on the Collaboration Agent Manager server.
7. Go to the directory `/var/mcp/media/avica` on the Collaboration Agent Manager server.
8. Type `unzip AacpaOtv-client-f-g.zip AacpaOtv/* —d fmgtemp/` and press **Enter**.
9. Type `cp -R fmgtemp/AacpaOtv/* /var/mcp/media/prov_pa_installs/otv` and press **Enter**.
10. Type `rm -rf fmgtemp` and press **Enter**.
11. Copy the file `AccWebCustomerConfig.xml` file to the directory `/var/mcp/media/prov_pa_installs/otv/` on the Collaboration Agent Manager server.
12. At the prompt, type `chown -R ntappsw:ntappgrp /var/mcp/media/prov_pa_installs/otv` and press **Enter**.
13. At the prompt, type `chmod -R 770 /var/mcp/media/prov_pa_installs/otv` and press **Enter**.

### Next steps

Proceed to Enabling Audio/Video in Collaboration Agent in the Provisioning Manager on page 540.

#### Related links

Audio/Video in Collaboration Agent on page 518

## Enabling Audio/Video in Collaboration Agent in the Provisioning Manager

As one of the final steps in the configuration of Audio/Video in Collaboration Agent, you must enable the feature in the Provisioning Manager.

### Before you begin

Complete the steps in Installing the Audio/Video in Collaboration Agent client software on page 539.

### About this task

You must enable

### Procedure

1. In the Provisioning Client window, select **System Manager** > **Location Setting**.
2. Select **AViCA Enabled**.
3. Click **Save**.

### Example

### Next steps

Proceed to Verifying integration of the multimedia client software with Collaboration Agent on page 541.

#### Related links

Audio/Video in Collaboration Agent on page 518

## Verifying integration of the multimedia client software with Collaboration Agent

### About this task

Use this procedure to verify that the Audio/Video in Collaboration Agent client software is integrated with Collaboration Agent.

### Procedure

1. Open your web browser and go to `https://<Collaboration Agent Manager IP address or FQDN>/aacpa`.

   The Avaya Aura Conferencing Collaboration Agent login page appears.
2. Log into Collaboration Agent.
3. Enter a conference.

   The Audio/Video in Collaboration Agent popup dialog box should appear, indicating that the Audio/Video in Collaboration Agent client software is integrated properly with Collaboration Agent.

#### Related links

Audio/Video in Collaboration Agent on page 518

## Hardening Audio/Video in Collaboration Agent

The following checklist provides a high-level view of the tasks involved in hardening Audio/Video in Collaboration Agent.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Create a certificate for the Flash Media Gateway IP address that is signed by Avaya Aura® System Manager. | See Creating a System Manager- signed certificate for the Flash Media Gateway IP address on page 543. | | |
| 2 | Create a VeriSign-signed certificate for the Flash Media Gateway FQDN. | See Creating a VeriSign-signed certificate for the Flash Media Gateway on page 543. | | |
| 3 | Secure the JMX connection between the Flash Media Gateways and the RTMPS connection to the Flash Media Gateway server. | See Securing the JMX connection between the Flash Media Gateways and the RTMPS connection to the Flash Media Gateway Management server on page 545. | | |
| 4 | Configure a SIP TLS connection from the Flash Media Gateway to the Avaya Aura® Session Manager. | See Configuring a secure SIP TLS connection from the Flash Media Gateway to Avaya Aura Session Manager on page 546. | | |
| 5 | Configure a secure RTMPS connection between the Flash Media Gateways and the Audio/Video in Collaboration Agent clients. | See Configuring a secure RTMPS connection between the Flash Media Gateways and the Audio/ Video in Collaboration Agent clients on page 547. | | |

**Related links**

Audio/Video in Collaboration Agent on page 518

Creating a System Manager- signed certificate for the Flash Media Gateway IP address on page 543

Creating a VeriSign-signed certificate for the Flash Media Gateway on page 543

Securing the JMX connection between the Flash Media Gateways and the RTMPS connection to the Flash Media Gateway Management server on page 545

Configuring a secure SIP TLS connection from the Flash Media Gateway to Avaya Aura Session Manager on page 546

Configuring a secure RTMPS connection between the Flash Media Gateways and the Audio/Video in Collaboration Agent clients on page 547

## Creating a System Manager- signed certificate for the Flash Media Gateway IP address

### About this task

Use the following procedure to create a certificate for the Flash Media Gateway IP address that is signed by System Manager.

### Procedure

1. Log on to System Manager.
2. Click **Services** > **Security**.
3. In the navigation pane, click **Certificates** > **Authority**.
4. In the navigation pane, click **Add End Entity**.
5. In the Add End Entity window, complete the following fields:
    - **End Entity Profile**: Select **INBOUND_OUTBOUND_TLS** from the list.
    - **Username**: Enter the IP address of the Flash Media Gateway.
    - **Password**: Enter any password. You will use this password when creating the certificate.
    - **Confirm Password**: Type the password again.
    - **CN, Common Name (first entry)**: Enter the userID for the specific administrator. For example, admin.
    - **Token**: Select **JKS file** from the list.
6. Click **Add End Entity**.
7. In the navigation pane, click **Public Web**.
8. In the navigation pane of the new browser window or tab, click **Create Keystore**.
9. Type the user name and password, and click **OK**.
10. Click **OK**.
11. Click **OK**, and save the *.jks file on your PC.

**Related links**

Hardening Audio/Video in Collaboration Agent on page 542

## Creating a VeriSign-signed certificate for the Flash Media Gateway

### About this task

Use this procedure to create a VeriSign-signed certificate for the Flash Media Gateway FQDN to make it accessible in the Internet.

## Procedure

1. Log on to the Flash Media Gateway server as `ntsysadm` through ssh or directly on the server console.
2. Enter **`su -`** to log on as root.
3. At the prompt `password`, type the root password, and press **Enter**.
4. At the prompt, type `mkdir /var/mcp/fmg/certs/external` and press **Enter**.
5. At the prompt, type `cd /var/mcp/fmg/certs/external` and press **Enter**.
6. Type `openssl genrsa -des3 -out <FMG_FQDN>.key 2048` and press **Enter** to create a private key.

   **Note:**

   The value 2048 represents the bit length of the key.
7. When prompted, enter a password, and press **Enter**.
8. Type `openssl req -new -key <FMG_FQDN>.key -out <FMG_FQDN>.csr -subj “/C=<country>/O=<company>/ST=<state>/L=<location>/CN=<FMG_FQDN>”` to create a private key.

   An example is `openssl req -new -key FMGServer1@avaya.com.key -out FMGServer1@avaya.com.csr -subj “/C=US/O=Avaya, Inc./ST=Colorado/L=Westminster/CN=FMGServer1@avaya.com”` where `FMGServer1@avaya.com` is the *<FMG_FQDN>*.
9. Press **Enter** to create the private key.
10. Submit the CSR file to VeriSign to get a certificate.
11. Obtain the appropriate VeriSign root and intermediate CA certificates.
12. Put the CA certificates and the Flash Media Gateway certificate returned from VeriSign in the directory `/var/mcp/fmg/certs/external` on the server.
13. Type `cd /var/mcp/fmg/certs/external` and press **Enter**.
14. Type `cat VeriSign_G5_top.crt VeriSign_G3_Int.crt <FMG_FQDN>.cer > <FMG_FQDN>.chain.crt` and press **Enter** to create the certificate chain.
15. Type `openssl pkcs12-export -out <FMG_FQDN>.p12 -inkey <FMG_FQDN>.key -in <FMG_FQDN>.chain.crt` and press **Enter** to create the p12 keystore that contains the Flash Media Gateway certificate chain and the private key.
16. When prompted, enter the password you entered in Step 1.
17. When prompted, enter the new export password.
18. Type `cp <FMG_FQDN>.p12 ../` and press **Enter** to copy the p12 keystore to the directory `/var/mcp/fmg/certs`.

19. Type /var/mcp/run/fmg/bin/convertP12toJKS and press **Enter** to convert the p12 keystore to a JKS keystore.
20. Follow the instructions. When prompted for a password, enter the export password you entered in Step 16.
21. Transfer the file *<FMG_FQDN>*.jks from the directory /var/mcp/fmg/certs to your PC.

### Next steps

If you want to verify your steps, you can check the jks contents using the following command:

```
/usr/java/latest/bin/keytool -list -v -keystore keystore.jks
```

**Related links**

Hardening Audio/Video in Collaboration Agent on page 542

## Securing the JMX connection between the Flash Media Gateways and the RTMPS connection to the Flash Media Gateway Management server

### About this task

Use this procedure to secure:

- the JMX connection between the Flash Media Gateways
- the RTMPS connection to the Flash Media Gateway Management server

### Procedure

1. Log on to the Flash Media Gateway server as ntsysadm through ssh or directly on the server console.
2. Enter **su -** to log on as root.
3. At the prompt password, type the root password, and press **Enter**.
4. Put the *.jks keystore in the directory /var/mcp/fmg/certs. You created this *.jks keystore in Creating a System Manager- signed certificate for the Flash Media Gateway IP address on page 543.
5. Go to the directory /var/mcp/run/fmg/bin.
6. Type installKeystore and press **Enter**.
7. Follow the instructions.

   **Note:**

   Select the option to install the keystore for All Management Interfaces.
8. When finished, type service red5 restart and press **Enter** to restart the Audio/Video in Collaboration Agent server software.

**Related links**

Hardening Audio/Video in Collaboration Agent on page 542

## Configuring a secure SIP TLS connection from the Flash Media Gateway to Avaya Aura® Session Manager

### About this task

Use this procedure to configure a secure SIP TLS connection from the Flash Media Gateway to Avaya Aura® Session Manager.

### Procedure

1. Log on to System Manager and create a TLS SIP entity link from Session Manager to each Flash Media Gateway using port 5061.
2. Open a web browser and go to `https://<PROV IP address or FQDN>:8443/fmgadmin/index.html` where <PROV IP address or FQDN> is the IP address or FQDN of the server running Provisioning Manager.

   The Log On page for Avaya One Touch Video 3.0 appears.
3. In the User Name box, enter `admin`.
4. In the Password box, enter `admin01`.
5. Click **Log on**.

   The Legal Notice page appears.
6. On the Legal Notice page, read the information provided.
7. To accept the information displayed, click **Accept**.

   The Welcome page appears.
8. From the Flash Media Gateway area in the navigation panel, click **List All**.
9. In the System Status area of the Flash Media Gateway page, select a Flash Media Gateway, and click **Edit**.
10. In the SIP Trunk area, change the port from 5060 to 5061, and click **Save**.
11. Repeat Steps 9 and 10 for each Flash Media Gateway.
12. From the Cluster area in the navigation panel, click **List All**.
13. In the System Status area of the Flash Media Gateway page, select a cluster, and click **Edit**.
14. In the SIP Trunk area, make the following changes:
    - Port: Set to `5061` (or other port that is used for SIP TLS on Session Manager).
    - Enable: Set to **TRUE**.
    - TLS certificate: Click Upload, select the certificate you create in Creating a System Manager- signed certificate for the Flash Media Gateway IP address on page 543 and upload the file.
    - Key Store Password: Enter the password from Step 3 in Creating a System Manager-signed certificate for the Flash Media Gateway IP address on page 543.

15. Click **Save**.
16. Go to the Flash Media Gateway on the Management Portal client and restart all Flash Media Gateways.

**Related links**

Hardening Audio/Video in Collaboration Agent on page 542

## Configuring a secure RTMPS connection between the Flash Media Gateways and the Audio/Video in Collaboration Agent clients

### About this task

Use this procedure to configure a secure the RTMPS connection between the Flash Media Gateways and the Audio/Video in Collaboration Agent clients.

### Procedure

1. Open a web browser and go to `https://<PROV IP address or FQDN>:8443/fmgadmin/index.html` where <PROV IP address or FQDN> is the IP address or FQDN of the server running Provisioning Manager.

   The Log On page for Avaya One Touch Video 3.0 appears.
2. In the User Name box, enter `admin`.
3. In the Password box, enter `admin01`.
4. Click **Log on**.

   The Legal Notice page appears.
5. On the Legal Notice page, read the information provided.
6. To accept the information displayed, click **Accept**.

   The Welcome page appears.
7. From the Flash Media Gateway area in the navigation panel, click **List All**.
8. In the System Status area of the Flash Media Gateway page, select a Flash Media Gateway, and click **Edit**.
9. In the General area, make the following changes:
   - RTMPS Certificate: Click **Upload**, select the certificate you created in Creating a VeriSign-signed certificate for the Flash Media Gateway on page 543, and click **Open**.
   - RTMPS JKS Password: Enter the password from Creating a VeriSign-signed certificate for the Flash Media Gateway on page 543.
10. Click **Save**.
11. Restart the Flash Media Gateway.
12. Repeat Steps 7 through 11 for each Flash Media Gateway.
13. From the Settings area in the navigation panel of the Avaya One Touch Video 3.0 application, click **Customer Configuration**.

The ACC Web Customer Configuration page appears.

14. From the Cluster box, select the cluster that you created. This is the primary address that the Audio/Video in Collaboration Agent client will use to connect to the Flash Media Gateways.
15. From the Protocol box, select **rtmps**. The Audio/Video in Collaboration Agent client will use RTMPS to establish connections across the Flash domain.
16. From the Profile Name box, select the profile that you created.
17. From the Meetme Route Name box, select the MeetMe conferencing route that you created. This is the route that the Audio/Video in Collaboration Agent client will use to connect callers to a MeetMe conference.
18. From the Event Route Name box, select the Event conferencing route that you created. This is the route that the Audio/Video in Collaboration Agent client will use to connect callers to an Event conference.
19. Check the **Audio Available** check box if you want to make the audio capability available to the Audio/Video in Collaboration Agent client using this configuration. This option is available only if licensed.
20. Check the **Video Available** check box if you want to make the video capability available to the Audio/Video in Collaboration Agent client using this configuration. This option is available only if licensed.
21. Check the Default Audio Selected check box if you want to make the audio capability available by default to the Audio/Video in Collaboration Agent client using this configuration.
22. Check the Default Video Selected check box if you want to make the video capability available by default to the Audio/Video in Collaboration Agent client using this configuration.
23. Click **Generate** to create the client configuration file (`AccWebCustomerConfig.xml`).

    The Configuration Text dialog box appears and displays the contents of the `AccWebCustomerConfig.xml`.
24. Click **Save**.
25. Using the Select location for download by dialog box, specify where you want to save the file `AccWebCustomerConfig.xml`, and then click **Save**.
26. Click **Log Off** at the top of the page to log off Avaya One Touch Video 3.0.
27. Log on to the Collaboration Agent Manager server as `ntsysadm` through ssh or directly on the server console.
28. Enter **`su -`** to log on as root.
29. At the prompt `password`, type the root password, and press **Enter**.
30. Copy the file `AccWebCustomerConfig.xml` file to the directory `/var/mcp/media/prov_pa_installs/otv/` on the Collaboration Agent Manager server.

31. At the prompt, type `chown -R ntappsw:ntappgrp /var/mcp/media/prov_pa_installs/otv` and press **Enter**.
32. At the prompt, type `chmod -R 770 /var/mcp/media/prov_pa_installs/otv` and press **Enter**.

**Related links**

Hardening Audio/Video in Collaboration Agent on page 542

## Upgrading Audio/Video in Collaboration Agent

If Avaya releases a new service pack or a new feature pack, you may have to upgrade the Audio/Video in Collaboration Agent feature. The process of upgrading the Audio/Video in Collaboration Agent feature is the same for service packs, feature packs, and patch releases. The only difference between these three types of releases is the method of obtaining the software from PLDS.

**Related links**

Audio/Video in Collaboration Agent on page 518

# Avaya Web Collaboration audio and video plug-in

Avaya Web Collaboration audio and video plug-in is a browser plug-in. Avaya are introducing this new client in this release of Avaya Aura® Conferencing.

**Related links**

Deploying Avaya Web Collaboration audio and video plug-in for internal access on page 549
Deploying Avaya Web Collaboration audio and video plug-in for external access on page 550
Audio/Video in Collaboration Agent on page 518
Deploying integrated audio and video on page 518

## Deploying Avaya Web Collaboration audio and video plug-in for internal access

You can deploy the Avaya Web Collaboration audio and video plug-in, in an internal-only enterprise environment. In this case, you only need to configure location mapping. Location mapping helps to determine the cascaded media server in a location that matches the user's IP address. If you do not configure location mapping, the internal user could end up streaming media to the conferencing host media server which may be in a faraway location. If your deployment does not have any cascading servers, then the Avaya Web Collaboration audio and video plug-in should operate successfully without any additional configuration.

For more information, see Configuring location mapping for the plug-in on page 550.

**Related links**

Avaya Web Collaboration audio and video plug-in on page 549

Configuring location mapping for the Avaya Web Collaboration audio and video plug-in on page 550

## Configuring location mapping for the Avaya Web Collaboration audio and video plug-in

The Avaya Web Collaboration audio and video plug-in uses a Collaboration Agent table for location mapping, rather than using Avaya Aura® Session Manager.

### About this task

Use this task to configure the location mapping for the Avaya Web Collaboration audio and video plug-in. If you do not configure a location, the Avaya Web Collaboration audio and video plug-in will attempt to use the default SBC that is configured in Element Manager. For more information, see Adding the SBC to the Element Manager on page 476.

### Procedure

1. In the Provisioning Client window, select **System Management > Routing > Locations**.
2. In the **Location Address Patterns** tab, from the **Select Location** drop-down menu, select a location.
3. In the **IP Address Pattern** field, add the IP pattern.
4. Click **Save**.

### Next steps

You can manage any existing locations using the table at the bottom of the **Location Address Patterns** tab.

**Related links**

Deploying Avaya Web Collaboration audio and video plug-in for internal access on page 549

# Deploying Avaya Web Collaboration audio and video plug-in for external access

If you wish to offer the Avaya Web Collaboration audio and video plug-in to users who reside outside of the enterprise firewall and if the Avaya Aura® Media Server (MS) resides within the enterprise firewall, you must configure a Session Border Controller (SBC). Avaya has tested and recommends the Avaya Session Border Controller for Enterprise (also known as the Sipera SBC) for use with the Avaya Web Collaboration audio and video plug-in.

You also require an SBC if you wish to offer the Avaya Web Collaboration audio and video plug-in to users who reside behind a Network Address Translation (NAT) hidden or private network.

For more information, see Deploying Avaya Web Collaboration audio and video plug-in for access by the public internet on page 461.

**Related links**

Avaya Web Collaboration audio and video plug-in on page 549

# Chapter 32: Securing your system using certificates

## Introduction to certificates

You can add security to your Avaya Aura® Conferencing system by using certificates to authenticate communications between the various servers. Certificates help to prove that server requests are authentic and trustworthy.

If you are unfamiliar with certificates or if you have not used them extensively before now, it can be useful to think of certificates in more familiar terms with an example from everyday life. The following table uses the example of a passport to introduce the concept of certificates. You will see this terminology throughout this chapter.

| Terminology | Everyday equivalent |
|---|---|
| A certificate signing request (CSR) | An application form for a passport |
| A public key | Your photograph |
| A private key | Your fingerprint (something which nobody else knows or could use) |
| The Certificate Authority (CA), for example, Thawte and Verisign | The passport office<br>If your deployment uses the Avaya Aura® architecture, Avaya also provides a Certificate Authority service using the System Manager application. So, in this scenario, System Manager is your ‘passport office’ or Certificate Authority from which you can obtain a passport. |
| The Identity certificate (server.crt) | The passport which has been sent by the passport office in response to your application form |
| The Certificate Authority (CA) certificate (ca.crt) | The receipt from the passport office, which proves that the passport is authentic |
| Keystore | The place where you store your passport. |
| Truststore | The place where you store your receipt from the passport office. |
| A .p12 or .pkx file.<br>This is also known as an X.509 certificate. | A file containing the passport and your finger print |

*Table continues…*

| Terminology | Everyday equivalent |
|---|---|
| OpenSSL | A publicly-available tool, which you can use to create:<br>• An application form for a passport<br>• A finger print<br>• A file containing the passport and the finger print |

So, essentially, you must take your photo and enter all of your details on a passport application form. You must then send the application form to the passport office to obtain your passport. When you receive your passport and receipt back from the passport office, you must show your passport, finger print, and receipt to your Avaya Aura® Conferencing system. Before your show them to your Avaya Aura® Conferencing system, you must package your passport and fingerprint into a single file. Sometimes, the fingerprint can have a password (also known as a passphrase) associated with it.

So, continuing with this example:

- Your passport is a document which helps people to identify you.
- Your passport receipt is proof that the issuer of the passport is authentic and official.
- Your fingerprint is the main proof of your authenticity. Your passport can be stolen and used by someone else. Only you can provide a live fingerprint.
- Your passphrase is like a glove which protects your fingerprint from being stolen.

**Related links**

Advanced information about certificates on page 553
Next steps for implementing security on page 555
Checklists for certificates on page 556

## Advanced information about certificates

The following sections contain reference information about certificates.

**Related links**

Introduction to certificates on page 552
Transport Layer Security on page 553
X.509 certificates on page 554
Cryptography on page 554

### Transport Layer Security

Avaya Aura® Conferencing uses the Transport Layer Security (TLS) protocol to prevent eavesdropping and tampering of communications sent across an IP network. The TLS protocol is comprised of two layers: the TLS Handshake protocol and the TLS Record protocol.

- The TLS Handshake protocol allows the server and client to authenticate each other using X.509 certificates and to negotiate an encryption algorithm and cryptographic keys.

- The TLS Record protocol performs symmetric cryptographic encryption and message integrity checks on the message payload.

**Related links**

Advanced information about certificates on page 553

## X.509 certificates

The use of the X.509 certificate is an integral part of TLS authentication. An X.509 certificate includes the private key of the server and general information that is pertinent to the owner (such as name and organization) in the subject Distinguished Name (DN) field of the certificate. The Common Name (CN) attribute of the DN identifies some unique name of the end-entity the certificate represents. For example, the CN can represent a Web server address such as CN=wcs1.domain.com. In addition, an independent Certificate Authority (CA) digitally signs each certificate. Any entity that has a copy of the CA certificate can use the CA certificate to validate the signature on the signed certificate.

The X.509 certificate is like a passport.

**Related links**

Advanced information about certificates on page 553

## Cryptography

The cryptography certificates support the following keys for the Certification Signature algorithm:

- 1024–bit, 2048–bit, and 4096–bit RSA asymmetric keys
- SHA-1 with RSA encryption
- SHA-256 with RSA encryption

**Table 30: HTTPS cipher suites**

| Cipher name | Enabled by default |
|---|---|
| SSL_RSA_EXPORT_WITH_DES40_CBC_SHA | no |
| SSL_RSA_EXPORT_WITH_RC4_40_MD5 | no |
| SSL_RSA_WITH_DES_CBC_SHA | no |
| SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA | no |
| SSL_RSA_WITH_3DES_EDE_CBC_SHA | no |
| SSL_RSA_WITH_RC4_128_MD5 | no |
| SSL_RSA_WITH_RC4_128_SHA | no |
| TLS_RSA_WITH_AES_128_CBC_SHA | yes |

**Table 31: Signaling cipher suites**

| Cipher name | Enabled by default |
|---|---|
| TLS_RSA_WITH_NULL_SHA | no |

*Table continues…*

| Cipher name | Enabled by default |
|---|---|
| TLS_RSA_WITH_AES_128_CBC_SHA | no |
| TLS_RSA_WITH_AES_256_CBC_SHA | yes |

**Table 32: SSH cipher suites**

**Note:**

You cannot make changes to the SSH cipher suites using the Avaya Aura® Conferencing Element Manager console. Instead, you can edit the `/etc/ssh/sshd_config` file, which is on each Avaya Aura® Conferencing server.

| Cipher name | Enabled by default |
|---|---|
| aes128-ctr | yes |
| aes192-ctr | yes |
| aes256-ctr | yes |
| arcfour256 | yes |
| arcfour128 | yes |
| aes128-cbc | yes |
| 3des-cbc | no |
| blowfish-cbc | no |
| cast128-cbc | no |
| aes192-cbc | no |
| aes256-cbc | no |
| arcfour | yes |

**Table 33: Secure audio and video cipher suites**

| Cipher name | Enabled by default |
|---|---|
| AES_CM_128_HMAC_SHA1_80 | yes |
| AES_CM_128_HMAC_SHA1_32 | no |

**Related links**

Advanced information about certificates on page 553

## Next steps for implementing security

In this release, the process of creating and importing security certificates is largely automated. In previous releases, the process was completely manual and required a large number of steps before you could provide single sign-on or secure conferencing. If you install Avaya Aura® Conferencing in an Avaya Aura® deployment, the various Avaya Aura® Conferencing network elements are already associated with certificates from System Manager. So, initially, System

Manager is the certificate authority (CA). For most deployments, you will not have to perform any additional tasks.

However, if you expand your system with additional network elements after initial installation, you must create and import certificates for these new network elements. Similarly, if you re-install or upgrade, you may be required to re-create and re-import certificates. Similarly, if you would like to use a different Certificate Authority (CA), you must perform some configuration tasks. If you would like to use a CA other than System Manager, you can easily configure an alternative CA after initial Avaya Aura® Conferencing installation and verification. The adoption of an alternative CA is appropriate for certain network elements such as the Web Conferencing Server (WCS) or if any network elements communicate with another external node such as an LDAP Directory Server that uses certificates signed by a third party. If you install Avaya Aura® Conferencing in a Turnkey deployment, you always use an alternative CA because there is no System Manager in your deployment.

**Note:**

For more information about Avaya Aura® System Manager, see *Administering Avaya Aura® System Manager*, which is available from the Avaya Support website: http://support.avaya.com.

**Related links**

Introduction to certificates on page 552

## Checklists for certificates

Ensure that you follow the correct sequence of tasks in the appropriate table. There are a number of task flows, depending on the features of your deployment. Decide which table is the right one for you:

- If you are using a third-party company as the Certificate Authority (CA), see Table 34: Third-party certificates on page 557. There are specialist companies which provide this service. Examples include Thawte and Verisign.
- If your deployment uses System Manager as the Certificate Authority (CA), without the Avaya Aura® Session Border Controller, see Table 35: System Manager certificates  on page 557.
- If your deployment uses System Manager as the Certificate Authority (CA), with Avaya Aura® Session Border Controller, see Table 36: System Manager certificates with Avaya Aura Session Border Controller (Avaya SBCE) on page 558.

## Third-party certificates

**Table 34: Third-party certificates**

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Generate a private key | Generating a private key on page 559 | | |
| 2 | Generate a certificate signing request (CSR) | Generating a Certificate Signing Request on page 560 | Send this request to the third-party company which you are using as the Certificate Authority (CA). In response, you will receive a server certificate and a Certificate Authority certificate. | |
| 3 | Create a .p12 or .pkx file | Creating a PKCS#12 file on page 561 | This is a bundle file which contains the private key and the server certificate. | |
| 4 | Import the Certificate Authority (CA) certificate | Importing CA certificates from a third party Certificate Authority  on page 562 | | |
| 5 | Import the Identity certificate | Importing identity certificates from a third party Certificate Authority on page 563 | | |

## System Manager certificates

**Table 35: System Manager certificates**

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Find out your enrollment password | Obtaining an enrollment password from System Manager on page 564 | | |
| 2 | Create certificates for each network element | Creating identity certificates signed by System Manager on page 564 | | |
| 3 | Import each certificate to each network element | Importing a new identity certificate for the Web | | |

*Table continues…*

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| | | Conferencing Server on page 573<br>Importing a new identity certificate for the Avaya Aura Media Server on page 568<br>Importing a new identity certificate for the Provisioning Manager on page 571<br>Importing a new identity certificate for the Web Conferencing Management Server on page 573<br>Importing a new identity certificate for the Element Manager on page 570<br>Importing a new identity certificate for the Collaboration Agent Manager on page 571<br>Importing a new identity certificate for the Application Server on page 567 | | |

## System Manager certificates in an Avaya Aura® Session Border Controller (Avaya SBCE) deployment

**Table 36: System Manager certificates with Avaya Aura® Session Border Controller (Avaya SBCE)**

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Generate a certificate signing request (CSR) using the server FQDN. | Creating a Certificate Signing Request on page 574 | For example, for the Collaboration Agent server, enter the Collaboration Agent FQDN in the **Common Name** field. The CSR | |

*Table continues…*

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| | | | consists of two files.<br>• .csr<br>• .key | |
| 2 | Using the System Manager administrative interface, generate a certificate. | Creating an end entity on page 575 | Enter a username and password for the certificate and make a note of these details. | |
| 3 | Sign the certificate. | Creating the certificate by using certificate signing request on page 576 | Sign the certificate using the username and password which you have just entered in the previous task and copy and paste the content of the .csr file which you generated in the first task. | |

**Related links**

Introduction to certificates on page 552

# Securing your system using third-party certificates

## Generating a private key

### About this task

Use the following procedure to generate a new RSA private key to use with a Certificate Signing Request (CSR).

### Procedure

On a system that has OpenSSL installed, type **`openssl genrsa -des3 -out <private key filename>.key 2048`**, and press **Enter**.

**Note:**

The value 2048 represents the bit length of the key. For certificates created via OpenSSL, the bit length is typically 2048. You can choose other values such as 1024 or 4096. The value is dependent on the security policy of your network.

### Result

A file with the name <private key filename>.key containing the encrypted key is created.

### Next steps

Proceed to Generating a Certificate Signing Request.

## Generating a Certificate Signing Request

### Before you begin

You must have previously generated or have access to an RSA private key that is associated with the certificate.

### About this task

Use the following procedure to create a Certificate Signing Request (CSR) to send to the appropriate CA for signing.

### Procedure

1. Update the `/etc/pki/tls openssl.cnf` file, as follows:

```
[ v3_req ]

# Extensions to add to a certificate request
extendedKeyUsage = clientAuth,serverAuth
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment

[ req ]
default_bits                                           = 2048
default_md                                            = sha256
default_keyfile            = privkey.pem
distinguished_name                        = req_distinguished_name
attributes                                                = req_attributes
x509_extensions        = v3_ca      # The extentions to add to the self signed
cert

# Passwords for private keys if not present they will be prompted for
# input_password = secret
# output_password = secret

# This sets a mask for permitted string types. There are several options.
# default: PrintableString, T61String, BMPString.
# pkix          : PrintableString, BMPString (PKIX recommendation before 2004)
# utf8only: only UTF8Strings (PKIX recommendation after 2004).
# nombstr : PrintableString, T61String (no BMPStrings or UTF8Strings).
# MASK:XXXX a literal mask value.
# WARNING: ancient versions of Netscape crash on BMPStrings or UTF8Strings.
string_mask = utf8only

req_extensions = v3_req # The extensions to add to a certificate request
```

2. Type **`openssl req -new -key <private key filename>.key -out <csr filename>.csr -subj "/C=US/O=My Org/CN=<FQDN>"`**, and press **Enter**.

   ✱ **Note:**

   The <FQDN> is the only part that is required for certificates used by Avaya Aura® Conferencing. For all other fields of the subject name of the certificate, check with your Enterprise Public Key Infrastructure group or the Public Certificate Authority where you send the request for signing.

### Result

A file with the name <csr filename>.csr containing the Certificate Signing Request is created.

### Next steps

Proceed to creating a PKCS#12 file.

## Creating a PKCS#12 file

### Before you begin

You must have access to the following:

- the private key
- the pass phrase that protects the private key
- the certificate that has been signed by the CA (an Identity certificate)

### About this task

Use the following procedure to create a PKCS#12 file containing the signed certificate and private key pair.

### Procedure

On the system that has OpenSSL installed, type **`openssl pkcs12 -export -out <certificate filename>.p12 -inkey <private key filename>.key -in <certificate filename>.crt`**.

### Result

A file with <certificate filename>.p12 containing the certificate and private key is created.

## Removing the passphrase key file

### About this task

Optional: For Document Conversion Server installation. Use the following procedure to remove a passphrase from the passphrase protected key file.

### Procedure

On a system that has OpenSSL installed, type `openssl rsa -in <protected private key filename>.key -out <unprotected private key filename>.key`, and press **Enter**.

### Result

A passphrase protected key file is removed.

## Importing CA certificates from a third party Certificate Authority

The CA certificate is like a receipt for your passport. The Certificate Authority (passport office) sends the CA certificate to you along with your server certificate (passport) in response to your Certificate Signing Request (CSR) (passport application).

Privacy Enhanced Mail (PEM) Base64 encoded DER or binary DER file formats are supported. The format is one of the following filename extensions: .pem, .cer, .crt, or .der.

The imported CA certificate must have a section entitled **X509v3 Authority Key Identifier** with the **keyid** field in it. You can check if your CA certificate has this required field using the free tool which is already installed on the Avaya Aura® Conferencing platform.

### Before you begin

You must have the Certificate Authority certificates in one of the previously mentioned formats that is accessible from the server where you launched the Element Manager Console.

### About this task

Use the following procedure to add an X.509 certificates to the Element Manager Truststore.

### Procedure

1. Use the OpenSSL tool to ensure that the CA certificate has a section entitled **X509v3 Authority Key Identifier** with the **keyid** field.
    a. On a system that has OpenSSL installed, type `openssl x509 -in <certificate file> -text` in the command line.
    b. Check the resulting certificate description to ensure that the required section is present.
2. Log on to the Element Manager Console.
3. In the navigation pane of the Element Manager Console, select **Security** > **Certificate Management** > **Truststore**.
4. In the Truststore window click **Add (+)**.
5. In the **Select File** dialog box, select the file containing the certificate you wish to import into the Truststore.
6. Click **Open**.
7. Click **OK**.
8. Repeat this procedure for any additional CA certificates that are required.
9. Restart the Avaya Media Server (AMS) network element.

### Next steps

If you are using additional, intermediate certificates, you can use the same procedure to add them.

## Importing identity certificates from a third party Certificate Authority

The identity certificate is like a passport. Before you import it to your system, you must bundle it up with your private key. The certificate and the private key must be contained in a PKCS#12 file when you import it into the Keystore.

These certificates are acquired from a third party Certificate Authority (CA), for example, VeriSign or your enterprise Certificate Authority. The benefit of using certificates signed by a third party Certificate Authority is that the signing Certificate Authority is usually already installed on most Web browsers. This allows users to access the various Web components of the system without having to handle browser security warnings or to figure out how to install the appropriate CA certificates onto your clients.

❗ **Important:**

Some client devices do not function properly when the required CA certificates are not configured in the client trust store. If you are using a client device that is not directly supported by the enterprise, Avaya recommends that you use a well-known trusted CA.

### Before you begin

You must have the following:

- A PKCS#12 file that contains the signed certificate and private key.
- Access to the PKCS#12 file from the workstation where you launch the Element Manager Console.
- The password used to access the contents of the file.

✳ **Note:**

For information about creating the PKCS#12 file, see Creating a PKCS#12 file on page 561.

### About this task

Use the following procedure to import identity certificates from a third party Certificate Authority.

### Procedure

1. Log on to the Element Manager Console.
2. In the navigation pane, select **Security** > **Certificate Management**.
3. Click **Keystore**.
4. In the Keystore window, click **Add (+)**.

5. In the **Add PKCS#12 File** dialog box, complete the following fields:
    - **Logical Name**: Type a logical name for the certificate to be assigned to a specific managed network element, for example, CA1Cert.
    - **PKCS#12 File**: Click **Browse** and select the PKCS#12 file that contains the certificate key pair to import.
    - **Password**: Type the password used to protect the PKCS#12 file.
    - **Export Password**: Type the password used to protect the PKCS#12 file
6. Click **Apply**.

# Securing your system using System Manager certificates

## Obtaining an enrollment password from System Manager

If you are using System Manager as your Certificate Authority, there is already a 'passport receipt' stored in the Truststore. This is like a ca.crt.

To generate new server certificates (passports) for each network element in your deployment, you require a piece of information from System Manager called an Enrollment Password.

### About this task

Use the following procedure to obtain the enrollment password.

### Procedure

1. Log on to System Manager.
2. On the System Manager console, click **Services** > **Security**.
3. In the navigation pane, click **Certificates**.
4. Click **Enrollment Password**.
5. On the Enrollment Password screen, in the **Existing Password** field, record the password for use in the following procedure.
6. On the Security tab, click **x** to close the Security window.

### Next steps

Proceed to Creating identity certificates signed by System Manager on page 564.

## Creating identity certificates signed by System Manager

Use this task to create ‘passports’ or certificates for each separate network element. Sometimes network elements can have the same certificate. For example, in a simplex system, where the

Collaboration Agent server and the Provisioning Manager server reside on the same server, you can use the same certificates for both servers.

#### Before you begin

You must know the enrollment password as completed in Obtaining an enrollment password from System Manager on page 564.

#### About this task

Use the following procedure to create X.509 Certificates signed by the System Manager for any Network Elements created after the initial installation, or to create new certificates when necessary.

#### Procedure

1. In the navigation pane of Element Manager Console, click **Security > Certificate Management > Enrollment Request**.
2. In the Certificate Enrollment window, complete the following fields:
   - **Logical Name**: Type a logical name for the certificate to be assigned to a specific managed network element, for example, Provisioning Manager NE.
   - **Bit length**: Select 1024, 2048, or 4096 from the list. If your security policy does not specify bit length, select **2048**.
   - **Common name**: Type the FQDN or IP address, for example, emsvc.avaya.com. See Guidelines for certificate configuration on page 566 for guidance on common name values for certificates that use the System Manager as the Certificate Signing Authority.
   - **Enrollment password**: This password must match the current Enrollment Password that is configured on System Manager.
3. Click **Submit**.
4. Repeat these steps for each network element that resides on a separate server.

#### Result

The certificate is automatically installed on the Element Manager Keystore.

**Note:**

Prior to certificate expiry, Avaya recommends that you generate a new certificate using a new logical name and then refresh the certificate by changing the network element to use the new logical name. The expired certificate can then be removed from the Element Manager Keystore.

#### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

#### Related links

Guidelines for certificate configuration on page 566

## Guidelines for certificate configuration

Use the following table to figure out the values required for each field when you are creating certificates for each network element.

The Network Elements that require certificates to be signed by the System Manager Certificate Authority can also be signed by another Certificate Authority instead, for example, an intermediate enterprise Certificate Authority. In this situation, the System Manager CA is configured as an intermediate Certificate Authority of an Enterprise Certificate Authority.

**Important:**

If the System Manager Certificate Authority is mentioned, there must be a trust relationship between that Network Element and the System Manager.

**Note:**

If TLS is enabled for the SIP interfaces, TLS must be enabled on each of the SIP interfaces as shown in the following table. Avaya recommends that you deploy the system with TLS enabled and is enabled by default.

**Note:**

If you are using a reverse proxy in your deployment, then third party certificates are not installed on Avaya Aura® Conferencing.

**Table 37: Guidelines for certificates**

This table lists the configuration guidelines for large deployments. The footnotes show the differences for SMB and medium enterprises.

| Network Element | Network Element interface | Certificate Authority | Logical Name | Common Name |
|---|---|---|---|---|
| Element Manager | EM Internal OAM | System Manager | EMIntOAMCert | FQDN of service address |
| | EM External OAM | N/A | N/A | N/A |
| Provisioning Manager | Prov Internal OAM HTTPS | System Manager | EMS1-PROV-FQDN-CERT | FQDN of server address |
| | Prov External OAM HTTPS | N/A | N/A | N/A |
| | CA Directory Server | System Manager | EMS1-PROV-FQDN-Cert | FQDN of server address |
| | CA HTTPS | Enterprise/Public/System Manager | EMS1-CA-FQDN-Cert | FQDN of server address |
| | CA SIP | System Manager | EMS1-IP-Cert | IP address of server address |
| Collaboration Agent | CA HTTPS | Enterprise/Public/System Manager | MWCS1-FQDN-Cert | FQDN of server address |

*Table continues…*

| Network Element | Network Element interface | Certificate Authority | Logical Name | Common Name |
|---|---|---|---|---|
|  | CA Directory Server | System Manager | MWCS1-FQDN-Cert | FQDN of server address |
|  | CA SIP | System Manager | MWCS1-IP-Cert | IP address of server address |
| Application Server | AS SIP | System Manager | ASSIPCert | IP address of the service address |
|  | AS Directory Server |  | ASSIPCert | IP address of the service address |
| Media Server | Media Server SIP | System Manager | MWCS1-IP-CERT[10] | IP address of server address |
|  | Media Server SOAP |  | MWCS1-IP-CERT[10] |  |
| Document Conversion Server | DCS HTTPS | System Manager | DCSS1-FQDN-Cert[11] | FQDN of server address |
| Web Conferencing Management Server | WCMS HTTPS | System Manager | EMS1-IP-Cert | IP address of server address |
| Web Conferencing Server[12] | WCS HTTPS | Enterprise/Public/ System Manager | WCS1Cert | FQDN of service address or wildcard. An example wildcard is *.mydomain.com |

### Related links

Creating identity certificates signed by System Manager on page 564

## Importing a new identity certificate for the Application Server

Use this task to import a certificate into an application server network element.

### Before you begin

- A new certificate for the Application Server must exist in the Element Manager Keystore.

[10] For SMB and medium size deployments, use the existing EMS1-FQDN-Cert and EMS2-FQDN-Cert.

[11] For SMB and medium size deployments, use the existing EMS1-IP-Cert and EMS2-IP-Cert.

[12] If you are using a third party Certificate Authority to generate certificates, the certificate for the WCS network element must support the following Certificate Key Usages:

- Signing
- Key encipherment
- Web Server Authentication
- Web Client Authentication

- The certificate has been signed by a Certificate Authority that the System Manager trusts. This is typically the System Manager Certificate Authority.

**Note:**

If the Application Server is online, it will require a restart of the Network Element Instance afterwards.

### About this task

Use the following procedure to assign a certificate to the Application Server.

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Application Servers**.
2. In the Application Servers window, select **AS1**.
3. Click **Edit (-/+)**.
4. In the Edit Application Server dialog box, complete the following field:
    - **SIP Certificate**: If the **Enable SIP TLS** option is enabled, select the required SIP certificate by logical name, for example, ASSIPCert
5. Click **Apply**.

## Importing a new identity certificate for the Avaya Aura® Media Server

### Before you begin

- A new certificate for each Avaya Aura® Media Server must exist in the Element Manager Keystore.
- The new certificate has been signed by a Certificate Authority that is in the Element Manager Truststore.
- The Avaya Aura® Media Server is in the Offline State.

### About this task

Use the following procedure to assign a new certificate the Avaya Aura® Media Server.

### Procedure

1. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers**.
2. In the Media Servers window, select **MS1**.
3. Click **Edit (-/+)**.

4. In the Edit Media Server dialog box, complete the following fields:
    - **SIP Certificate**: If the **SIP TLS** option is enabled, select the required SIP certificate from the list. This list corresponds to the logical names in the Keystore, for example, AMS1Cert.
    - **SOAP Certificate**: If the **Enable SOAP/TLS** option is enabled, select the appropriate certificate form the list. This list corresponds to the logical names in the Keystore. Generally, the same certificate used for the SIP interface is used here, for example, AMS1Cert.
5. Click **Apply**.

## Importing a new certificate for the DCS

### Before you begin

- A new certificate for the Document Conversion Server (DCS) must exist in the Element Manager Keystore.
- The certificate has been signed by a Certificate Authority that is in the Element Manager Truststore. This is typically the System Manager Certificate Authority.

### About this task

Use the following procedure to assign a new certificate to the DCS.

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Document Conversion Servers** > **Document Conversion Servers**.
2. In the Document Conversion Servers window, select the DCS, for example, **DCS1**.
3. Click **Edit (-/+)**.
4. In the Edit DCS dialog box, complete the following field:
    - **HTTPS Certificate**: Select the required certificate from the list. This list corresponds to the logical names in the Keystore, for example, DCSS1-FQDN-Cert.

      **Note:**

      This certificate must be based on the FQDN, not the IP address.
5. Click **Apply**.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

**Related links**

Deploying and starting the new DCS on page 270

## Importing a new identity certificate for the Element Manager

### Before you begin

- A new certificate for the Element Manager must exist in the Element Manager Keystore.
- Single sign-on from the System Manager to the Element Manager Console requires that the certificate has the FQDN of the EM Service address as the Common Name of the certificate.
- The certificate has been signed by a CA that the System Manager trusts. This is typically the System Manager CA.

**Note:**

The Element Manager Network Instance will require a restart afterwards.

### About this task

Use the following procedure to assign a new certificate to the Element Manager.

### Procedure

1. Log on to the Element Manager Console.
2. In the navigation pane of Element Manager Console, click **Feature Server Elements > Element Manager**.
3. In the Element Manager window, select the element manager.
4. Click **Edit (-/+)**.
5. In the Edit Element Manager dialog box, complete the following:
    - **Enable HTTP Port**: Clear this check box.
    - **Internal OAM – HTTPS Certificate**: Select the required HTTPS certificate by logical name, for example, EMIntOAMCert.
6. Click **Apply**.
7. Click **File** > **Exit** on the Element Manager Console to exit.
8. Log on to EMServer with an account using the AA role, such as, `ntappadm`, through SSH or directly at the server console.
9. At the password prompt, type the password for ntappadm.
10. Type `emStop.pl`, and press **Enter**.
11. Type `emStart.pl`, and press **Enter**.
12. Log on to the Element Manager Console.
13. **(Optional)** If the new certificate is signed by a different Certificate Authority not previously trusted by the Element Manager Console, an Element Manager Authentication Dialog window appears. Select **Store the certificate's signing certificate authority as a trusted certificate for this and future connections**

14. Click **Apply**.

## Importing a new identity certificate for the Collaboration Agent Manager

This procedure is specific to large deployments with redundancy and large simplex deployments. If you have an SMB or a medium deployment with redundancy or an SMB or a medium deployment simplex deployment, you can skip this procedure. The large deployment layouts make use of independent Collaboration Agent Manager Network Elements to provide support for physical separation from the Provisioning Manager Network Element for security and scalability.

### Before you begin

Certificates for the Collaboration Agent Manager must exist in the Element Manager Keystore.

**Note:**

If Collaboration Agent Manager is online, it will require a restart of the Network Element Instance afterwards.

### About this task

Use the following procedure to assign a certificate to the Collaboration Agent Manager.

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Collaboration Agent**.
2. In the Collaboration Agent Managers window, select **CA1**.
3. Click **Edit (-/+)**.
4. In the Edit Collaboration Agent dialog box, complete the following fields:
   - **Enable HTTP Port**: Clear the check box.
   - **CA HTTPS Certificate**: Select the required HTTPS certificate by logical name, for example, CA1Cert.
   - **SIP Certificate**: If the **Enable SIP TLS Port** option is enabled, select the required SIP certificate by logical name, for example, CA1SIP.
5. Click **Apply**.

## Importing a new identity certificate for the Provisioning Manager

### Before you begin

- A certificate for the Provisioning Manager must exist in the Element Manager Keystore.
- Single sign-on from the System Manager to the Provisioning Manager requires that the certificate has the FQDN of the server hosting the Provisioning Manager as the Common Name.

- The certificate has been signed by a CA that the System Manager trusts. This is typically the System Manager CA.

**Note:**

If the Provisioning Manager is online, it will require a restart of the Network Element Instance afterwards.

### About this task

Use the following procedure to assign a certificate to the Provisioning Managers.

### Procedure

1. Log on to the Element Manager Console.
2. In the navigation pane of Element Manager Console, click **Feature Server Elements > Provisioning Managers**.
3. In the Provisioning Managers window, select the **PROV1**.
4. Click **Edit (-/+)**.
5. In the Edit PROV1 dialog box, complete the following fields:

   In the Prov section:

   - **Enable HTTP Port**: Clear the check box.
   - **Internal OAM HTTPS Certificate**: Select the required HTTPS certificate by logical name, for example, Prov1IntOAMCert.

   In the CA section:

   - **Enable HTTP Port**: Clear the check box.
   - **HTTPS Certificate**: Select the required HTTPS certificate by logical name, for example, PA1Cert.
   - **SIP Certificate**: If the **Enable SIP TLS Port** option is enabled, select the required SIP certificate by logical name, for example, PA1SIPCert.

   **Note:**

   The certificates in the PA submenus are required only when the PA is co-hosted with the Provisioning Manager.
6. Click **Apply**.
7. Repeat this procedure for any additional Provisioning Managers.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

## Importing a new identity certificate for the Web Conferencing Management Server

### Before you begin

- A new certificate for the Web Conferencing Management Server must exist in the Element Manager Keystore.
- The certificate has been signed by a Certificate Authority that is in the Element Manager Truststore. This is typically the System Manager Certificate Authority.

### About this task

Use the following procedure to assign a new certificate to the Web Conferencing Management Server.

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Management Servers**.
2. In the Web Conferencing Manager Servers window, select **WCMS1**.
3. Click **Edit (-/+)**.
4. In the Edit Web Conferencing Manager Server dialog box, complete the following field:
   - **HTTPS Certificate**: Select the required certificate from the list. This list corresponds to the logical names in the Keystore, for example, EMS1-IP-Cert.
5. Click **Apply**.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

## Importing a new identity certificate for the Web Conferencing Server

### Before you begin

A new certificate with a common name using the FQDN of the Web Conferencing Server must exist in the Element Manager Keystore.

✳ **Note:**

If the Web Conferencing Server is online, it will require a restart of the Network Element Instance afterwards.

### About this task

Use the following procedure to assign a new certificate to the Web Conferencing Server.

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Servers**.
2. In the Web Conferencing Server window, select **WCS1**.
3. Click **Edit (-/+)**.
4. In the Edit Web Conferencing Server dialog box, complete the following field:
    - **HTTPS Certificate**: Select the required HTTPS certificate by logical name, for example, WCS1Cert.
5. Click **Apply**.
6. Repeat this procedure for any additional Web Conferencing Servers.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

# Securing your system using System Manager certificates in an Avaya SBCE deployment

## Creating a Certificate Signing Request

### Procedure

1. Log in to the Avaya SBCE EMS web interface with administrator credentials.
2. In the left navigation pane, click **TLS Management** > **Certificates**.

   The system displays the Certificates screen.
3. Click **Generate CSR**.

   The system displays the TLS Management Generate CSR window.
4. Enter the appropriate information in the TLS Management Generate CSR screen, and click **Generate CSR**.

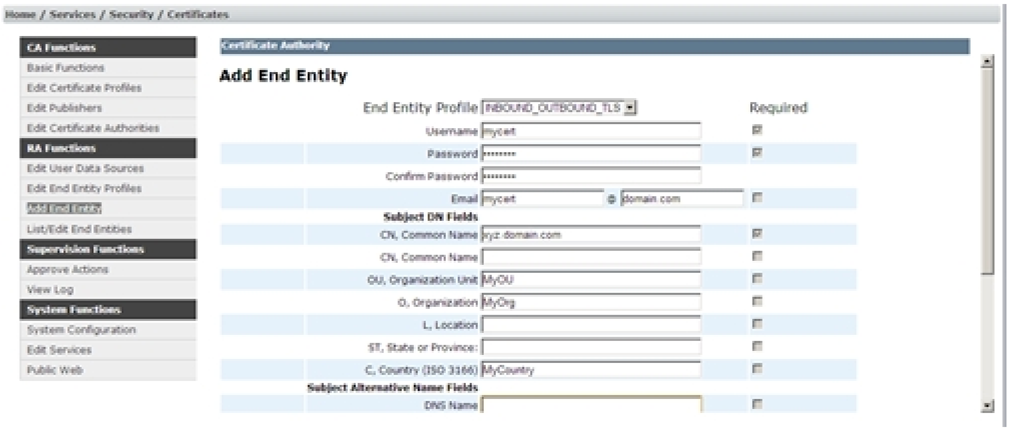
   Ensure that the **Key Encipherment** and **Digital Signature** check boxes are selected. Do not clear these check boxes.

## Creating an end entity

### Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. Click **RA Functions** > **Add End Entity**.
4. On the Add End Entity page, in **End Entity Profile**, click **INBOUND_OUTBOUND_TLS**.
5. Type the username and password.

   The password is mandatory for each end entity. Without the password, you cannot generate the certificate from System Manager because you require the password to authenticate the certificate generation request.
6. Complete the fields that you want in your certificate.



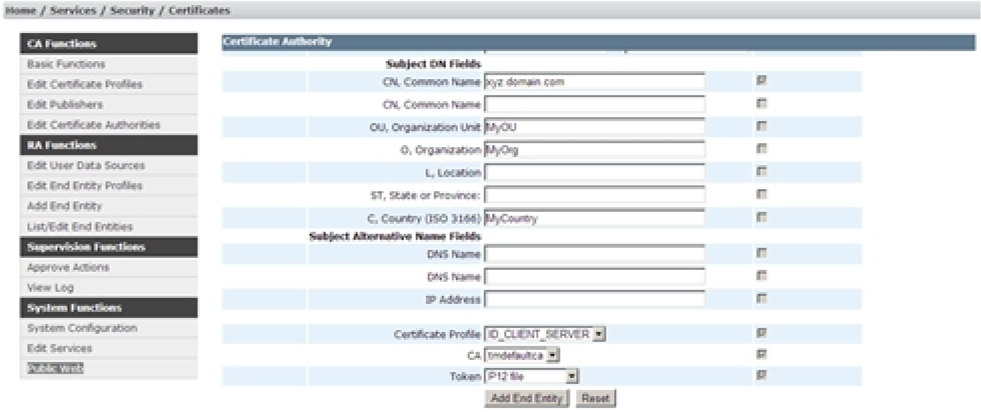
Add End Entity

| | | |
|---|---|---|
| End Entity Profile | INBOUND_OUTBOUND_TLS | Required |
| Username | mycert | ☑ |
| Password | •••••••• | ☑ |
| Confirm Password | •••••••• | |
| Email | mycert @ domain.com | □ |
| **Subject DN Fields** | | |
| CN, Common Name | xyz.domain.com | ☑ |
| CN, Common Name | | □ |
| OU, Organization Unit | MyOU | □ |
| O, Organization | MyOrg | □ |
| L, Location | | □ |
| ST, State or Province: | | □ |
| C, Country (ISO 3166) | MyCountry | □ |
| **Subject Alternative Name Fields** | | |
| DNS Name | | □ |

The system automatically selects the following:

- **ID_CLIENT_SERVER** in **Certificate Profile**
- **tmdefaultca** in **CA**
- **User Generated** in **Token**

  With **User Generated**, the system generates the certificate by using CSR. You can also select **P 12 file**.



| | | |
|---|---|---|
| **Subject DN Fields** | | |
| CN, Common Name | xyz domain com | ☑ |
| CN, Common Name | | ☐ |
| OU, Organization Unit | MyOU | ☐ |
| O, Organization | MyOrg | ☐ |
| L, Location | | ☐ |
| ST, State or Province: | | ☐ |
| C, Country (ISO 3166) | MyCountry | ☐ |
| **Subject Alternative Name Fields** | | |
| DNS Name | | ☐ |
| DNS Name | | ☐ |
| IP Address | | ☐ |
| Certificate Profile | ID_CLIENT_SERVER | ☑ |
| CA | tmdefaultca | ☑ |
| Token | P12 file | ☑ |

7. Click **Add End Entity**.

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

## Creating the certificate by using certificate signing request

### Before you begin

Create an end entity.

For more information, see Creating an end entity.

### Procedure

1. On the System Manager web console, click **Services** > **Security**.
2. In the left navigation pane, click **Certificates** > **Authority**.
3. In the left navigation pane, click **Public Web**.
4. On the public EJBCA page, click **Enroll** > **Create Certificate from CSR**.
5. To get your certificate, on the Certificate Enrollment from a CSR page, do the following:
   a. Enter the same username and the password that you provided while creating the end entity.
   b. In the text box, paste the PEM-formated PKCS10 certification request.
   c. Click **OK**.

      The system signs the certificate signing request (CSR) and generates a PEM-formatted certificate that contains the values provided in the end entity.

# Securing the administration GUIs in your deployment

In addition to securing the various components of Avaya Aura® Conferencing to ensure secure usage of the product, you can also secure the various administrative interfaces to ensure secure administration of the product. For the most part, you can administer Avaya Aura® Conferencing using the Element Manager Console and the Provisioning Client. You can use the Element Manager Console to administer all of the network elements. You can use Provisioning Client to administer all of the users.

You can view alarms, logs, and Key Performance Indicators (KPIs) using the Element Manager Console. You can secure the access to these metrics using certificates.

**Table 38: Certificates for administrators**

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Create an end entity on System Manager | Creating an administrator entity for certificates from System Manager on page 577 | | |
| 2 | Install the certificate on the administrator's browser | Installing an identity certificate on the administrator's browser on page 578 | | |

**Related links**

Creating an administrator entity for certificates from System Manager on page 577

Installing an identity certificate on the administrator's browser on page 578

# Creating an administrator entity for certificates from System Manager

You must install a certificate on each administrator's Web browser to enable administrators to securely view the various alarms, logs, and Key Performance Indicators (KPIs) for the Avaya Aura® Media Server. You must define an End Entity for each administrator on the System Manager before the administrator can request a certificate from the System Manager.

## About this task

Use the following procedure to provision an End Entity for a certificate for an administrator Web browser signed by the System Manager.

## Procedure

1. Log on to System Manager.
2. Click **Services** > **Security**.

3. In the navigation pane, click **Certificates** > **Authority**.
4. In the navigation pane, click **Add End Entity**.
5. In the Add End Entity window, complete the following fields:
    - **End Entity Profile**: Select **OUTBOUND_TLS** from the list.
    - **Username**: Enter the user name for the specific administrator. For example, admin.
    - **Password**: Enter a password for the administrator. Use this password when creating the certificate.
    - **Confirm Password**: Type the password again.
    - **Email**: Type the email address of the administrator. For example, admin@mail.example-enterprise.com.
    - **CN, Common Name**: Enter the userID for the specific administrator. For example, admin.
    - **OU, Organization Unit**: Keep the default value. This value is based on the profile.
    - **O, Organization**: Keep the default value. This value is based on the profile.
    - **C, Country (ISO 3166)**: Keep the default value. This value is based on the profile.
    - **Certificate Profile**: Select **ID_CLIENT** from the list.
    - **CA**: Keep the default value. This value is based on the profile.
    - **Token**: Select **User Generated** from the list.
6. Click **Add End Entity**.
7. Repeat this procedure for each administrator who requires access.

**Related links**

Securing the administration GUIs in your deployment on page 577

## Installing an identity certificate on the administrator’s browser

### Before you begin

- A new End Entity has been created for the administrator.
- The username and password created for the end entity has been provided to the administrator.

### About this task

Use the following procedure to install the administrator identity certificate on the administrator browser.

**Note:**

You can create only one identity certificate for each username. If you use more than one computer or use both Firefox and Internet Explorer, then export the identity certificate and private key from the respective browser and install the identity certificate on the other computer or browser.

### Procedure

1. Log on to System Manager.
2. Click **Services** > **Security**.
3. In the navigation pane, click **Certificates** > **Authority**.
4. In the navigation pane, click **Public Web**.
5. In the navigation pane of the new browser window or tab, click **Create Browser Certificate**.
6. Type the Username and password, and click **OK**.
7. If the Web Access Confirmation dialog box appears, click **Yes** to allow the operation.
8. In the **Options** panel, click **OK**.
9. Choose from the following options:
    - If you are running Internet Explorer: In the Creating a new RSA signature key dialog box, click **OK**. In the VBScript: Certificate Management dialog box, click **OK**.
    - If you are running Mozilla Firefox: In the Alert dialog box, click **OK** to acknowledge that a new certificate has been installed.
10. Close the browser window or tab.

### Result

The identity certificate is installed on the Administrator Web browser.

#### Related links

Securing the administration GUIs in your deployment on page 577

# Chapter 33: Securing your recordings

## Introduction to secure recording

Avaya Aura® Conferencing captures audio and web collaboration within a conference. Avaya Aura® Conferencing does not record video and it does not record standalone web conferences (SWC). Standalone web conferences are conferences that do not have an Avaya Aura® Conferencing audio component. Instead, their audio component is provided by an external source, such as a direct call between two parties.

Avaya Aura® Conferencing does not implement a quota system. So, for example, the recordings of a single user could take up all of the available storage space.

Avaya Aura® Conferencing provides encryption for stored recordings on the hard drive. To enable encryption, you must choose encryption as an option at installation time. For more information, see, Encrypting the recording data disk on page 131. If you do not choose encryption as an option at installation time, recordings are stored and played back without encryption. In all cases, recordings are encrypted in transit, including for playback, assuming TLS encryption has been enabled for the system.

Users cannot edit recordings except to change the title, and they cannot search for a phrase within a recording.

For more information on configuring recording in your deployment, see Configuring the recording feature on page 339.

## Checklist for secure recordings

**Table 39: Checklist for secure recording**

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Ensure that you enable TLS when you install/add the recording (media) server. | In a small or medium deployment, the recording server is usually on the same server as the other | For more information on installing Avaya Aura® Conferencing, see Installing the AAC Platform on page 121. | |

*Table continues…*

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| | | Avaya Aura® Conferencing network elements.<br>Encrypting the recording data disk on page 131<br>In a large deployment, the recording server is usually on a dedicated server.<br>Adding a media server dedicated for recording on page 342 | | |
| 2 | Configure a certificate for the recording server. | Creating identity certificates signed by System Manager on page 564 and Importing a new identity certificate for the Avaya Aura Media Server on page 568<br>or<br>Creating and importing a certificate for the dedicated recording server on page 345 | For more information on certificates, see Introduction to certificates on page 552. | |

# Adding a media server dedicated for recording

## About this task

Use this procedure to add a media server that will be dedicated for recording.

**Note:**

During this procedure, you will create a new media server cluster. A media server cluster supports a maximum of eight media servers:

- one primary
- one secondary
- six standard servers

## Procedure

1. In the navigation pane of Element Manager Console, click **Addresses**.
2. In the Addresses window, click **Add (+)**.

3. In the Add IPv4 Address dialog box, enter the logical name and IP address for the media server.
4. Click **Apply**.
5. In the navigation pane of Element Manager Console, click **Servers**.
6. In the Servers window, click **Add (+)**.
7. In the Add Server dialog box, complete the following fields:
    - **Short Name**
    - **Long Server Name**
    - **Internal OAM (Default) Address**: Enter the IP address you specified in Step 3.
    - **Operating System**: Select **linux**.
    - **Host Name**: Enter the short name or FQDN of the server.
8. Click **Apply**.
9. In the navigation pane of Element Manager Console, click **Feature Server Elements > Media Servers and Clusters > Media Servers**.
10. In the Media Servers window, click **Add (+)**.
11. In the Add Media Server dialog box, complete the following fields:
    - **Short Name**
    - **Long Name**
    - **Base Port**: Type 49000.
    - **Enable SIP TCP**: Select this check box to enable.

      **OR**

      **Enable SIP TLS**: Select this check box to enable.
    - **SIP Certificate**: If SIP TLS is enabled, select the certificate you want to use for SIP TLS. For more information, see the chapter for Configuring Transport Layer Security.

    **Note:**

    Accept the default for all other fields.
12. Click **Apply**.
13. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers** > **<media server you specified in Step 3> Instance**.
14. In the Media Server Instance window, click **Add (+)**.
15. In the Add Media Server Instance dialog box, complete the following fields:
    - **Server**: Select the media server you created in Step 3.
    - **Load or Patch**: Select the software load.

- **Engineering**: Select the configuration that corresponds to your hardware type and layout.

16. Click **Apply**.
17. In the navigation pane of Element Manager Console, click **Feature Server Elements > Media Servers and Clusters > Media Server Clusters**.
18. In the Media Server Clusters window, click **Add (+)**.
19. In the Add Media Server Cluster dialog box, complete the following fields:
    - **Short Name**
    - **Long Name**
    - **Primary Server**: Select the Avaya Aura® Media Server network element. This list contains only the media server network elements that do not belong to any cluster. You must specify a primary server.
    - **Secondary Server**: If this cluster has two or more Avaya Aura® Media Servers, you must specify a secondary server. Otherwise, leave this field blank.
    - **Role**: Select **RECORDING ONLY**.
20. Click **Apply**.
21. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers** > **MediaServer2** >**NE Maintenance**.
22. In the Media Server Maintenance dialog box, select the row for ID 0.
23. Click **Deploy**.

    The Maint state changes from **None** to **Deploying**, indicating that the deploy process is in progress. After the deploy process is complete, the Maint state changes to **None**, and the Admin state changes from **Configured** to **Offline**.
24. Click **Start**.

    The Maint state changes from **None** to **Starting**, indicating that the start process is in progress. After the activation process is complete, the Maint state changes to **None**, and the Admin state changes from **Offline** to **Online**.

    Check the state transitions for the following fields:

    | Field | Status |
    |---|---|
    | Maint | None |
    | Admin | Online |
    | Link | Up |
    | Oper | Active |

25. In the navigation pane of Element Manager Console, click **Feature Server Elements > Media Servers and Clusters > Media Server Clusters**.
26. In the Media Server Clusters window, select **MediaServer1**, and click **Edit (+/-)**.

27. In the Edit Media Server Cluster dialog box, make sure the Role box is set to **CONFERENCING ONLY** .

**Related links**

Dedicated recording server deployment only on page 342

## Creating and importing a certificate for the dedicated recording server

### Before you begin

You must know the enrollment password as completed in Obtaining enrollment password from System Manager on page 564.

### About this task

Use this procedure to create a new certificate for the dedicated Recording server. This procedure creates a passport for the server and assumes that the System Manager is acting as the passport office. If you are using another authority as the passport office, see Introduction to certificates on page 552.

### Procedure

1. In the navigation pane of Element Manager Console, click **Security** > **Certificate Management** > **Enrollment Request**.
2. In the Certificate Enrollment window, complete the following fields:
    - **Logical Name**: Type a logical name for the certificate to be assigned to the dedicated Recording server (for example, AMS2Cert).
    - **Bit length**: Select 1024, 2048, or 4096 from the list. If your security policy does not specify bit length, select **1024**.
    - **Common name**: Type the IP address.
    - **Enrollment password**: This password must match the current Enrollment Password that is configured on System Manager.
3. Click **Submit**.

    The certificate is automatically installed on the Element Manager Keystore.
4. In the navigation pane of the Element Manager Console, select **Feature Server Elements** > **Media Servers and Clusters** > **Media Servers**.
5. In the Media Servers window, select the dedicated Recording server.
6. Click **Edit (-/+)**.
7. In the Edit Media Server dialog box, complete the following fields:
    - **SOAP/TLS checkbox**: Enable this checkbox.

- **SIP TLS checkbox**: Enable this checkbox.
- **SIP Certificate**: Select the certificate you created from the list. This list corresponds to the logical names in the Keystore (for example, AMS2Cert).
- **SOAP Certificate**: Select the certificate you requested from the list. This list corresponds to the logical names in the Keystore (for example, AMS2Cert).

8. Click **Apply**.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

**Related links**

Dedicated recording server deployment only on page 342

# Chapter 34:  Securing your audio and video

In addition to securing your Avaya Aura® Conferencing network elements, GUI interfaces, and recordings, you can secure your audio and video communications.

You can secure your audio and video communications using Secure Real Time Protocol (SRTP). This section describes how to configure Audio and Video SRTP with Avaya Aura® Conferencing.

This feature enables users to conduct secure audio conferences if all participants in the conference are using SRTP audio. This feature also enables users to conduct secure video conferences if all participants in the conference are using SRTP video.

## Endpoints supported with Audio SRTP

The following endpoints support Audio SRTP:

- Avaya 9600 Series IP Deskphones 96x1 H.323 Release 6.2
- Avaya 9600 Series IP Deskphones 96x1 H.323 Release 6.3
- Avaya 9600 Series IP Deskphones 96x1 SIP Release 6.2
- Avaya 9600 Series IP Deskphones 96x1 SIP Release 6.3
- Avaya Communicator Release 2.0 for Windows (TLS only)
- Avaya Communicator Release 2.0 for iPad Devices
- Avaya one-X Communicator Release 6.1
- Avaya one-X Communicator Release 6.1.1
- Avaya one-X Communicator Release 6.1.6
- Avaya one-X Communicator Release 6.2

## Endpoints supported with Video SRTP

The following endpoint supports Video SRTP:

- Avaya one-X Communicator Release 6.2 (SIP)
- Avaya Communicator Release 2.0 for Windows

### Related links

Audio and Video SRTP configuration tasks on page 587
Administering the SRTP settings for Avaya Aura Conferencing on page 587
Modifying Communication Manager settings for SRTP on page 591

# Audio and Video SRTP configuration tasks

You must perform the following tasks to use audio and video SRTP with Avaya Aura® Conferencing.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Configure TLS to secure the connection between Session Manager and Avaya Aura® Conferencing. | See Configuring TLS route to Session Manager from the Element Manager on page 311. | Ensure that **Enable SIP TLS Port** is selected in the Transport Information area in the **Add/Edit Session Manager** dialog box. | |
| 2 | Configure TLS for Avaya Media Server connections. | See Next steps for implementing security on page 555. | For each Avaya Media Server, ensure that **Enable SIP TLS** is selected in the Transport area in the **Add/Edit Media Server** dialog box. | |
| 3 | Configure the SRTP settings for audio and video on Avaya Aura® Conferencing. | See Administering the SRTP settings for Avaya Aura Conferencing on page 587. | | |
| 4 | Configure Communication Manager to support audio and video SRTP with Avaya Aura® Conferencing. | See Modifying Communication Manager settings for SRTP on page 591. | | |

**Related links**

Securing your audio and video on page 586

# Administering the SRTP settings for Avaya Aura Conferencing

## About this task

Use this procedure to configure the SRTP settings for audio and video for Avaya Aura® Conferencing.

Here are the recommended Audio SRTP settings when configuring Avaya Aura® Conferencing in the Aura Solution:

- Security Policy - **BEST EFFORT**
- Encrypt RTCP - Disabled (that is, check box is not selected)

- Video Allowed For Security Enforced Calls - N/A
- Enforce SIPS for Security Enforced Calls - Enabled
- Enable Video Encryption - Enabled
- Mode - AES_CM_128_HMAC_SHA1_32:
    - Priority - **2**
    - Send Lifetime - Disabled (that is, check box is not selected)
    - SRTP Master Key Lifetime - **31**
    - Key Derive Rate - **0**
    - Master Key Index Length - **0**
- Mode - AES_CM_128_HMAC_SHA1_80:
    - Priority - **1**
    - Send Lifetime - Disabled
    - SRTP Master Key Lifetime - **31**
    - Key Derive Rate - **0**
    - Master Key Index Length - **0**

### Procedure

1. In the navigation pane of Element Manager Console, select **Security > SRTP Settings**.
2. In the SRTP Settings dialog box, configure each setting. For more information, see SRTP Settings dialog box field descriptions on page 588.
3. When finished, click **Apply**.

### Related links

Securing your audio and video on page 586
SRTP Settings dialog box field descriptions on page 588

## SRTP Settings dialog box field descriptions

| Name | Description |
|---|---|
| Security Policy | Select the type of media security policy you want to use. The security policy you specify dictates the type of media (audio and video)Avaya Aura® Conferencing will include in offer SDPs and how Avaya Aura® Conferencing generates answer SDP during SDP negotiation. Choices are:<br>• **BEST EFFORT**<br>When this option is selected, Avaya Aura® Conferencing will generate requests using SIPS and will offer both RTP and SRTP media using capability negotiation. If the request fails because SIPS is not supported by the endpoint, |

*Table continues…*

| Name | Description |
|---|---|
| | Avaya Aura® Conferencing will retry the request using SIP and RTP. Avaya Aura® Conferencing will accept and negotiate RTP-only offers, SRTP-only offers, and RTP/SRTP best effort offers. SRTP will be negotiated where allowed when a compatible SRTP crypto suite is offered. RTP will be negotiated for RTP-only offers and for RTP/SRTP best effort offers when a compatible SRTP crypto suite is not offered.<br>• **SECURITY DISABLED**<br>When this option is selected, Avaya Aura® Conferencing will support only RTP. Avaya Aura® Conferencing will accept and generate RTP offers/answers. Avaya Aura® Conferencing will negotiate to RTP when it receives a request that contains an SDP offer with RTP media or best-effort media. Avaya Aura® Conferencing will reject requests that contain an SDP offer with only SRTP media by replying with a 480 Temporarily Unavailable response. A local treatment will be played to the end user.<br>• **SECURITY ENFORCED**<br>When this option is selected, Avaya Aura® Conferencing will support only SRTP media. Avaya Aura® Conferencing will negotiate to SRTP media when it receives a request that contains an SDP offer with SRTP media or best-effort media and a compatible crypto suite. Avaya Aura® Conferencing will reject requests that contain an SDP offer with only RTP media by replying with a 480 Temporarily Unavailable response. A local treatment will be played to the end user.<br>**Note:**<br>The SECURITY ENFORCED option does not guarantee signaling security. To ensure full encryption, you must configure TLS for the Avaya Aura® Conferencing Application Server network element. |
| Encrypt RTCP | Select this check box to indicate that Avaya Aura® Conferencing supports encrypted SRTCP messages.<br>When not selected, Avaya Aura® Conferencing indicates the preference to send and receive unencrypted SRTCP messages by including the UNENCRYPTED_SRTCP session parameter in outgoing offers. When selected, Avaya Aura® Conferencing supports sending and receiving encrypted SRTCP messages. Avaya Aura® Conferencing will not include the UNENCRYPTED_SRTCP session parameter in its offers. In either case, if the UNENCRYPTED_SRTCP session parameter is received in an offer, Avaya Aura® Conferencing will echo the UNENCRYPTED_SRTCP session parameter in its answer, and unencrypted SRTCP will be used in both directions. If the UNENCRYPTED_SRTCP session parameter is not received in an offer, Avaya Aura® Conferencing will not include the UNENCRYPTED_SRTCP session parameter in the answer and encrypted SRTCP is used in both directions. |
| Video Allowed For Security Enforced Calls | Select this check box if you want Avaya Aura® Conferencing to send secure audio and unsecure video while the **Security Policy** field is set to SECURITY ENFORCED. |

*Table continues…*

| Name | Description |
|---|---|
| | If this check box is not selected, Avaya Aura® Conferencing will disable the video port for calls with secure audio. This field only takes effect if the **Security Policy** field is set to SECURITY ENFORCED. |
| Enforce SIPS for Security Enforced Calls | Select this check box if you want to require incoming calls to use SIPS signaling to negotiate secure media for the call. In addition, Avaya Aura® Conferencing generated requests with SRTP-only media offers will use SIPS signaling. |
| Enable Video Encryption | Select this check box if you want to enable secure video for your configuration. If you do not select this check box, Avaya Aura® Conferencing does not provide secure video transmission. In other words, if you do not select this check box, Avaya Aura® Conferencing provides unencrypted video. |
| Mode | Select the encryption mode(s) you want to use. This is commonly referred to as the “crypto suite.“ Choices are **AES_CM_128_HMAC_SHA1_32** and **AES_CM_128_HMAC_SHA1_80**. |
| Priority | Select the priority for the associated mode. Choices are **0** to **9**.<br>If you want to disable the encryption mode, select **0**. A non-zero value indicates the priority that should be applied to the crypto suite during media negotiation. **1** is the highest priority; **9** is the lowest priority. |
| Send Lifetime | Select this check box to indicate that Avaya Aura® Conferencing should include the Master Key Lifetime specified by the SRTP Master Key Lifetime option (below) in the key parameter of the SRTP crypto attribute during SRTP media negotiation. When not selected, the Master Key Lifetime field is not included in the key parameter of the SRTP crypto attribute during SRTP media negotiation. In this case, the default lifetime for the crypto suite is used for media negotiation. |
| SRTP Master Key Lifetime | Specify the maximum number of SRTP packets that will use a particular master key. Choices are **1** to **31**. |
| Key Derive Rate | Specify how frequently a new session key is derived from an SRTP master key. Choices are **0** to **24**. |
| Master Key Index Length | Specify the size of the Master Key Index/Identifier (MKI) field in the actual SRTP packets. Choices are **0** to **4**. An MKI is used to identify the master key from which the session key that authenticates the particular packet was derived. When set to **0**, Avaya Aura® Conferencing will not include an MKI value and its associated length in the key parameter of the SRTP crypto attribute during SRTP media negotiation, and an MKI field will not be included in the actual SRTP packets. When the Master Key Index Length is set to a value greater than **0**, Avaya Aura® Conferencing will include an MKI value, and its associated length in the key parameter of the SRTP crypto attribute during SRTP media negotiation and an MKI field will be included in the actual SRTP packets. |

## Related links

Administering the SRTP settings for Avaya Aura Conferencing on page 587

# Modifying Communication Manager settings for SRTP

## About this task

Use the following procedure to modify Communication Manager settings to support Audio and Video SRTP. These settings are recommendations for “best effort.”

This section only applies to Avaya Aura® deployments. This section does not apply to Turnkey deployments.

## Procedure

1. Log on to System Manager as admin.
2. On the System Manager console, click **Elements >** Communication Manager.
3. In the navigation pane, click **Parameters > System Parameters – Customer Options**.
4. On the System Parameters – Customer Options page, select the appropriate device, and click **View**.
5. Click **Next Page** to go to page 4.
6. On page 4, verify **Media Encryption Over IP** is set to **Y**.

   ✱ **Note:**

   If **Media Encryption Over IP** is set to **N**, contact Avaya support.
7. In the navigation pane, click **Parameters > System Parameters – Features**.
8. On the System Parameters – Features page, select the appropriate device, and click **New**.
9. Click **Prev Page** to go to page 19.
10. In the IP Parameters section, set **Initial INVITE with SDP for secure calls** to **Y**.
11. Press **Enter** to save your changes.
12. In the navigation pane, click **Network > Signaling Groups**.
13. Click the check box of the appropriate signaling group, and click **Edit**.
14. On Page 1, set **Enforce SIPS URI for SRTP** to **Y**.
15. Press **Enter** to save your changes.
16. Log off System Manager.
17. Open your Web browser and in the Address bar, type the IP address for the Communication Manager System Management Interface (SMI).
18. At the Logon ID prompt, type your Logon ID, and click **Logon**.
19. Type your password, and click **Logon**.
20. Click the **Continue** button.
21. On the Administration menu, click **Native Configuration Manager**.
22. In the Server Login window, type your Logon ID, and click **OK**.

23. Type your password, and click **OK**.
24. In the Command field, type `change system-parameters ip-options`, and click **Send**.
25. On the IP-options system parameters page, click **NEXT PAGE** to navigate to page 2.
26. In the **Override ip-codec-set for SIP direct-media connections** field, type **n** if you are running Communication Manager 6.2 Feature Pack 3 or later.

    If you are running an earlier release of Communication Manager, type **y** in this field.
27. Click **Enter**.
28. In the Command field, type `change ip-codec-set #`, where `#` is the IP codec set you want to modify, and click **Send**.

    In default or new deployments, this is often `ip-codec-set 1` (and `ip-network-region 1`). If you are unsure, you should verify which IP network regions are being used in your deployment.
29. In the Media Encryption section on page 1 of IP Codec Set, perform the following steps:
    1. In field 1, type `1-srtp-aescm128-hmac80`.
    2. In field 2, type `2-srtp-aescm128-hmac32`.
    3. In field 3, type `none`.
30. Click **Enter**.
31. Repeat Steps 27 through 29 for each IP codec set.
32. When finished, close the Native Configuration Manager window.
33. In the Communication Manager system Management Interface (SMI) window, click **Logoff**.
34. Click **Log Off**.

**Related links**

Securing your audio and video on page 586

# Chapter 35: Hardening Avaya Aura® Conferencing for Avaya Aura® and Turnkey deployments

You should perform security hardening on the core servers (Element Manager servers and Avaya Media servers) of an Avaya Aura® Conferencing system after you install it or upgrade it. Avaya provides a number of advanced configuration options, which can add optimize the robustness of your security defence.

For maximum security, all scripts are run via the Linux sudo command to allow the scripts to access privileged devices without having to be the root user. You may be prompted to enter a password when running scripts mentioned in this chapter. If so, enter the administrator password (that is, ntsysadm, ntappadm, etc.) under which you are currently logged in, unless instructed otherwise.

## Configuring the BIOS password

Most planar BIOS provide the ability to configure an administrative password. If the BIOS on the server allows an administrative password to be configured, use the Administrator password, and refer to the server hardware installation guide for details on how to configure the BIOS password.

If the BIOS password can be configured, it must be configured on each server in the system.

**Note:**

A BIOS Power-On password is also available on most systems. However, because using the BIOS Power-On password can result in a service outage, use the BIOS administrative password. Do not configure a Power-On password.

## Configuring the BIOS boot order

For maximum security, you must set the BIOS boot order to **Hard Disk First, CD-ROM Second** for each server. For details on configuring the BIOS boot order, see the server hardware installation guide that was used to install the servers.

# Setting operating system inactive account auditing

### About this task

This task must be performed on all Element Manager servers and Avaya media servers.

### Procedure

1. Log onto the server as the *ntsysadm* user.
2. At the command prompt, enter **`configInactiveLoginAudit`** and press **Enter**.
3. At the prompt `Enter 'c' to configure, 'd' to display, or 'q' to quit [c/d/q]`, enter `c` to configure the audit, and press **Enter**.
4. At the prompt `Do you wish to enable Inactive Login Auditing? (Y/N) [Y]?`, enter `y` to turn on the audit, and press **Enter**.
5. At the prompt `Do you want to exempt any login accounts from the audit? (Y/N) [Y]?`, enter `y` to exempt login accounts from the audit, and press **Enter**.
6. Press **Enter** to accept the default list of exempted accounts.
7. At the prompt `Maximum number of inactive days before login account is locked`, press **Enter** to accept the default value for the number of days before account inactivity prior to account lock out.

# Configuring the operating system warning banners

Use this procedure to configure warning banners to display a message before users enter their user names and password, and another message after a successful log on. Warning banners typically state the legal implications of logging on to a system.

Following two warning banners are available in the platform:

- **/etc/issue** (displayed before login)

  **Note:**

  For SSH, the file **/etc/issue** is shown after users enter their user name and before they enter their password. This is considered a pre-login warning banner for SSH.

- **/etc/motd** (displayed after login)

To configure the operating system warning banners, perform the following steps:

1. Configure the pre-login warning banner. See Configuring the pre-login warning banner on page 595.
2. Configure the post-login warning banner. See Configuring the post-login warning banner on page 595.
3. Verify the warning banners. See Verifying the warning banners on page 595.

## Configuring the pre-login warning banner

### About this task

Use this procedure to configure the warning banner that is displayed before users enter their user names and passwords. This task must be performed on all Element Manager servers and Avaya Media Servers.

### Procedure

1. Log onto the server as the *ntsysadm* user.
2. At the command prompt, enter `vi /etc/issue` and press **Enter** to edit the pre-login banner.

   **Note:**

   You may use an editor other than *vi*.
3. Either cut and paste or type in the pre-login warning banner.
4. Save the file and exit the editor.

## Configuring the post-login warning banner

### About this task

Use this procedure to configure the warning banner that is displayed after the users log on successfully. This task must be performed on all Element Manager servers and Avaya Media Servers.

### Procedure

1. Log onto the server as the *ntsysadm* user.
2. At the command prompt, enter `vi /etc/motd` and press **Enter** to edit the post-login banner.

   **Note:**

   You may use an editor other than *vi*.
3. Either cut and paste or type in the post-login warning banner.
4. Save the file and exit the editor.

## Verifying the warning banners

### About this task

Use this procedure to verify the pre-login and post-login warning banners. For SSH, the pre-login banner is displayed after the you enter your user name and before you are prompted for your password. The post-login banner is displayed after you enter your password and before you are presented with a shell prompt.

### Procedure

1. Remotely access the server via SSH.
2. At the logon prompt, enter your user name and press **Enter**.

   The pre-login banner is displayed after the you enter your user name and before you are prompted for your password.
3. Enter your password and press **Enter**.

   The post-login banner is displayed after you enter your password.

   If the warning banners are not displayed after you configure them, contact the next level of support. Do not continue until you can verify the warning banners are displayed correctly.

## Configuring operating system password and account policies

### About this task

Use this procedure to configure the password complexity rules to ensure that user passwords are more secure. Password complexity rules apply only to subsequently configured passwords. This task must be performed on all Element Manager servers and Avaya Media Servers.

### Procedure

1. Log onto the server as the *ntsysadm* user.
2. At the command prompt, enter **`pwConfig`** and press **Enter**.
3. If you are prompted for your password, enter your password and press **Enter**.
4. At the prompt `Selection [1 to 5]` for the **Password Configuration Options** menu, enter `2` to select **Change Current Settings** and press **Enter**.
5. Using the values from the **OS Password and Account Settings** section, enter the appropriate value and press **Enter** at each prompt.
6. At the prompt `Press Enter to continue`, press **Enter**.
7. At the prompt `Selection [1 to 5]` for the **Password Configuration Options** menu, enter `4` to select **Save current settings to system files** and press **Enter**.
8. At the prompt `Press Enter to continue`, press **Enter**.
9. At the prompt `Selection [1 to 5]` for the **Password Configuration Options** menu, enter `5` to exit the menu and press **Enter**.

# Resetting the GRUB password

### About this task

Use this procedure to configure the Linux Grand Unified Bootloader (GRUB) password. The GRUB password prevents unauthorized access to the bootloader. Once the password complexity is configured, you must reset the GRUB password to comply with these new settings. This task must be performed on all Element Manager servers and Avaya Media Servers.

### Procedure

1. Log onto the server as the *ntsysadm* user.
2. At the command prompt, enter **`grubPWConfig`** and press **Enter**.
3. At the prompt `Enter 'c' to configure, 'd' to display, or 'q' to quit [c/d/q]`, enter `c` to configure the password and press **Enter**.
4. At the prompt `Enter the "bootloader" password`, enter a policy-compliant GRUB password and press **Enter**.
5. At the prompt `Enter the "bootloader" password again`, enter the GRUB password again and press **Enter**.

# Hardening the database

### About this task

This task must be performed on all servers that have the database installed.

### Procedure

1. Log onto the server as the *ntsysadm* user.
2. At the command prompt, enter **`hardenDb`** and press **Enter**.

# Configuring administrator accounts

## Creating new user-specific accounts

### About this task

This task must be performed for each OS administrator on each server. There should be at least one administrator per role on every system. The data mentioned in the following steps refers to the **OS Administrators** section from the **OS Hardening** tab of the Avaya Aura® Conferencing Intelligent Workbook.

## Procedure

1. Log onto the server as the *ntsysadm* user.
2. At the command prompt, enter **`userMgt`** and press **Enter**.
3. At the prompt `Enter Selection > (1 to 8)` for the **User Configuration Manager** menu, enter `1` to select **Add new user** and press **Enter**.
4. At the prompt `Please enter a user name [Between 6-30 chars]`, enter the *<role> username* and press **Enter**.
5. At the prompt `Enter Selection > (0,1000-10000) [0]`, press **Enter** to select the default value.
6. Enter the number for the appropriate role. The first role is the user's primary role. Separate multiple role entries with a comma (`,`).
7. Press **Enter**.
8. At the prompt `Would you like to continue (Y/N) [N]?`, enter `y` and press **Enter**.
9. At the prompt `Enter the <Role> username password` prompt, enter the initial password and press **Enter**.

   **Note:**

   This password is for initial login purposes only. The administrator will be required to change this password upon first login.
10. At the `Enter the <Role> username password` prompt, enter the initial password again and press **Enter**.
11. At the prompt `Would you like to add another user: (Y/N) [N]?`, enter `y` and press **Enter**.
12. Repeat steps 4 – 11 for the remaining OS administrators, selecting the appropriate role for each administrator. There should be only one role for each administrator.

    **Note:**

    All deployments do not use all roles that are available on the system. Add only those administrator accounts that are used in your deployment.

### Example

Following is an example of a system that contains the pre-configured users and newly created administrators.

| User | UID | Roles | Local Auth State | Sudo |
|---|---|---|---|---|
| [1] ntsysadm | 20229 | SSA | enabled | Y |
| [2] ntsecadm | 20230 | SA | enabled | N |
| [3] ntappadm | 20228 | AA | enabled | N |
| [4] ntbackup | 20231 | BA | enabled | N |

*Table continues…*

| User | UID | Roles | Local Auth State | Sudo |
|---|---|---|---|---|
| [5] ntdbadm | 20232 | DBA | enabled | N |
| [6] ntossadm | 20225 | OSS | enabled | N |
| [7] init | 20234 | SSA, AA, DBA | disabled | Y |
| [8] craft | 20235 | AA | disabled | N |
| [9] jackSSA | 20236 | SSA | enabled | N |
| [10] tonySA | 20237 | SA | enabled | N |
| [11] chloeAA | 20238 | AA | enabled | N |
| [12] allisonBA | 20239 | BA | enabled | N |
| [13] kimbDBA | 20240 | DBA | enabled | N |

# Allowing administrator sudo access

## About this task

In the pre-configured installation, the *ntsysadm* user is given full sudo access, which allows that administrator to become root. Only administrators with full sudo access can become root, so you should give this privilege only to administrators that can be trusted with this level of authority. Full sudo access can only be granted when the **userMgt** tool is run via the root user.

**Note:**

If the *ntsysadm* user is deleted before a new SSA is given full sudo access, you must run the script **userMgt** via the console (that is, the attached KVM) when logged in as the root user.

Use this task to configure the System Security Administrator (SSA) username with sudo capabilities.

## Procedure

1. Log onto the server as the *ntsysadm* user.
2. At the command prompt, enter **`su -`** and press **Enter**.
3. Enter the root password and press **Enter**.
4. Enter **`userMgt.pl`** and press **Enter**.
5. At the prompt `Enter Selection > (1 to 9)` for the **User Configuration Manager** menu, enter `6` to select **Sudo access management** and press **Enter**.
6. From the list of administrators, select the **System Security Administrator (SSA) username** and press **Enter**.
7. At the prompt `Would you like to continue (Y/N) [N]?`, enter `y` to continue and press **Enter**.
8. At the prompt `Would you like to allow/deny sudo for another user: (Y/N) [N]?`, enter `n` and press **Enter**.

# Loading a new authentication file

### About this task

After installation, the Client Services accounts are configured with the default authentication file. You must replace the default authentication file with the site-specific authentication file.

You must perform this task on each server.

### Procedure

1. Upload the new authentication file to the *ntsysadm* user.
2. Log onto the server as the *ntsysadm* user.
3. At the command prompt, type `loadauth -l` *`<new_authentication_file_pathname>`* and press **Enter**.

# Deleting pre-configured OS administrator accounts

### About this task

This task must be performed on each server.

✱ **Note:**

Before performing this procedure, make sure you have configured at least one user with the SSA role and sudo access. You must create at least one administrator per role on every system. For more information, see Creating new user-specific accounts on page 597.

### Procedure

1. Log onto the server using the System Security Administrator (SSA) username.

   ✱ **Note:**

   Do not login as *ntsysadm* because that administrator will be deleted in this procedure.

2. At the command prompt, enter **`userMgt`** and press **Enter**.
3. At the prompt `Enter Selection > (1 to 8)` for the **User Configuration Manager** menu, enter `2` to select **Delete a user** and press **Enter**.

   A list of all administrators on the system is displayed. You must delete the following administrators from the system via this menu:

   - ntsysadm
   - ntsecadm
   - ntappadm
   - ntbackup
   - ntdbadm

- ntossadm

4. When prompted to confirm the deletion of each user, enter `y` and press **Enter**.
5. At the **User Configuration Manager** menu, enter `5` to select **List users on this system** and press **Enter**.
6. Confirm that there are no pre-configured users listed. The only users listed should be those listed in **OS Administrators**.

### Example

Following is an example of a system where all pre-configured accounts except Avaya Services accounts have been deleted, an administrator for the five major roles has been created, and full sudo access has been provided to one SSA user.

| User | UID | Roles | Local Auth State | Sudo |
|---|---|---|---|---|
| [1] init | 20234 | SSA, AA, DBA | disabled | Y |
| [2] craft | 20235 | AA | disabled | N |
| [3] jackSSA | 20236 | SSA | enabled | Y |
| [4] tonySA | 20237 | SA | enabled | N |
| [5] chloeAA | 20238 | AA | enabled | N |
| [6] allisonBA | 20239 | BA | enabled | N |
| [7] kimbDBA | 20240 | DBA | enabled | N |

# Access Control List configuration

The Access Control List (ACL) configuration includes configuring the internal ACL rules and external ACL rules. The system uses the internal rules to apply to connections. Generate these rules by running the **`mcpGenIntACLconfig.pl`** program that creates the rules based on the configuration data in the Avaya Aura® Conferencing database. The external rules apply to restricting external access from ancillary devices to Avaya Aura® Conferencing. Configure the external rules manually.

Complete all tasks in *Configuring internal ACL rules* and *Configuring external ACL rules* to complete the ACL configuration. Avaya Aura® Conferencing applies the internal ACL rules only after you configure and commit the external ACL rules.

## Configuring internal ACL rules

### About this task

Use the following procedure to configure internal ACL rules.

### Procedure

1. Generate an internal ACL configuration file. See Generating an internal ACL configuration file on page 602.
2. Install an internal ACL configuration file on the primary Element Manager server. See Installing an internal ACL configuration file on the primary Element Manager server on page 602.
3. Install an internal ACL configuration file on all other servers. See Installing an internal ACL configuration file on all other servers on page 603.

## Generating an internal ACL configuration file

### Before you begin

You must be able to log onto the primary Element Manager server a user with the Application Administrator (AA) role.

### About this task

Use the following procedure to generate an internal ACL configuration file.

### Procedure

1. Log onto the primary Element Manager server as a user with the AA role.
2. At the command prompt, enter `cd /var/mcp/install` and press **Enter**.
3. Enter `mcpGenIntACLConfig.pl` and press **Enter**.

   The internal ACL configuration file has now been generated and resides on the primary Element Manager server. You must now install the internal ACL configuration file on all servers in the system (including the primary Element Manager server).

## Installing an internal ACL configuration file on the primary Element Manager server

### Before you begin

You must be able to log onto the primary Element Manager server as a user the System Security Administrator (SSA) role.

### About this task

Use the following procedure to install an internal ACL configuration file on the primary Element Manager server.

### Procedure

1. Log onto the primary Element Manager server as a user with the SSA role.
2. At the command prompt, enter `mcpInstIntACLConf -copy` and press **Enter**.

## Installing an internal ACL configuration file on all other servers

### Before you begin

You must be able to log onto the primary Element Manager server a user with the System Security Administrator (SSA) role.

### About this task

Use the following procedure to install an internal ACL configuration file on all other servers.

If your deployment supports integrated audio and video, this may include the Flash Media Gateway (FMG) server. For more information on integrated audio and video, see Deploying integrated audio and video on page 518.

### Procedure

1. Log onto the server as a user with the SSA role.
2. At the command prompt, enter `mcpInstIntACLConf` and press **Enter**.
3. At the prompt `Remote server IP address`, enter the primary Element Manager server internal OAM IP address and press **Enter**.
4. At the prompt `SFTP user id`, enter the SSA user name defined on the primary Element Manager server and press **Enter**.
5. At the prompt `SFTP password`, enter the SSA password and press **Enter**.
6. At the prompt `Please retype the password to confirm`, re-enter the SSA password and press **Enter**.
7. At the prompt `Confirm (Y or N)`, enter `y` and press **Enter**.

   ✻ **Note:**

   If you receive an error message that the remote host identification has changed, see *Deploying Avaya Aura® Conferencing* to fix the problem. Once you fix the keys, retry the script on this server.

8. Repeat Steps 1 through 7 on all remaining servers in the system.

   ✻ **Note:**

   The internal ACL rules are applied to the system only after you commit the ACL rules via the **iptcfg** tool. See Importing an external Access Control List configuration file on page 605.

## Configuring external ACL rules

### About this task

There are multiple methods available for configuring external ACL rules. The **iptcfg** tool provides an interactive menu that enables you to

- configure the settings for an individual node

- configure the settings for a port
- configure the DSCP settings
- import configuration files

The import files used in this section were auto-generated after the platform was installed. If the import file want not generated automatically, you must create that file manually.

When external ACL rules are committed via the **iptcfg** tool, the internal ACL rules file (previously installed) is used by the **iptcfg** tool to create firewall rules for the internal nodes. No further action is required to include the internal ACL rules.

Use the following procedure to configure external ACL rules.

### Procedure

1. If the Avaya Media Server is deployed on the target server, prepare the Avaya Media Server. See Preparing the Avaya Media Server on page 604.
2. Perform one of the following steps:
   - Create a configuration file and then import it using the **iptcfg** tool. See Importing an external ACL configuration file on page 605.
   - Configure the rules manually using the **iptcfg** tool. See Configuring external ACL rules manually (using the iptcfg tool) on page 606.
3. Verify the ACL configuration. See Verifying the ACL configuration on page 609.

## Preparing the Avaya Media Server

### Before you begin

- You must be able to log onto the server as a user with the System Security Administrator (SSA) role.
- You must know the root password.

### About this task

Perform this procedure on all servers where the Avaya Media Server is deployed, regardless of the layout type (that is, SMB, medium, or lrage)).

### Procedure

1. Log onto the server as a user with the SSA role.
2. At the prompt, enter `su -` and press **Enter**.
3. At the prompt password, enter the root password, and press **Enter**.
4. Enter `aacconfiginstall.pl` and press **Enter**.

   The following message is displayed:

   ```
   Install AAC configuration
   /var/mcp/ma/MAS/bin/chmodplat.sh
   /var/mcp/ma/MAS/bin/dscpconfig.sh install
   /var/mcp/ma/MAS/bin/dscpconfig.sh install
   ```

## Importing an external Access Control List configuration file

### About this task

Use this procedure to import an external Access Control List (ACL) configuration file. ACL configuration files are server specific, with each file containing IP addresses that are specific to a server. The Element Manager server and Avaya Aura® Media Server configuration files are different. The Avaya Aura® Media Server file has additional syntax. Refer to the appropriate example of the configuration files for each server. Log in as a root user and view examples of:

- The Avaya Aura® Media Server configuration file at `/opt/mcp/ipt/example` on Avaya Aura® Media Server.
- The Element Manager server configuration file, with instructions on how to configure the file, at `/opt/mcp/ipt/example` on the Avaya Aura® Conferencing server.

You might need to configure the following external trusted nodes in the configuration file:

- Remote syslog server
- Remote NTP server
- Administrator computer
- DNS

Perform this procedure on all servers in the Avaya Aura® Conferencing system.

### Procedure

1. Log on to the server as SSA.
2. At the prompt, enter `su -`, and press **Enter**.
3. At the password prompt, enter the root password, and press **Enter**.
4. Create an ACL configuration file based on the configuration file examples.

   Ensure that the trusted nodes listed in the configuration file contain the IP address of your computer. If your computer is not configured as a trusted node, you cannot access the server after you configure and commit the ACL rules because applying the rules will block access to the server.
5. To revert to the login as SSA, type `exit`, and press **Enter**.
6. After you create the ACL configuration file, type `iptcfg`, and press **Enter**.

   The system displays the **IPTables Configurations Options** menu.
7. At the prompt `Selection [1 to 9]`, enter `4` to select **Import Configurations**, and press **Enter**.

   The system displays a warning that the operation changes the IPTables rules.
8. At the prompt `Proceed (Y or N)`, enter `y` and press **Enter**.
9. At the prompt `Import file name (full path)`, enter the file path and the configuration file name of the server, and press **Enter**.

   The system displays the following warning:

```
WARNING: Trusted nodes must include those from which the user logs
into the current server to perform the maintenance tasks. If you
have not specified them as trusted nodes in the import file, you
will not be able to log in to the server again after the importing
has completed.
```

10. At the prompt `Proceed (Y or N)`, enter `y`, and press **Enter**.

## Configuring external ACL rules manually (using the iptcfg tool)

### Before you begin

You must be able to log onto the server as a user with the System Security Administrator (SSA) role.

### About this task

Use this procedure to configure the external ACL rules using the **iptcfg** tool. See External ACL configuration settings on page 609 to determine the list of trusted nodes, trusted ports, and DSCP settings you must configure on each server.

**Note:**

You must perform this procedure on all servers in the Avaya Aura® Conferencing system.

If your deployment supports integrated audio and video, this may include the Flash Media Gateway (FMG) server. For more information on integrated audio and video, see Deploying integrated audio and video on page 518.

### Procedure

1. Log onto the server as a user with the SSA role.
2. At the command prompt, enter `iptcfg` and press **Enter**.

   The IPTables Configurations Options menu appears.
3. At the prompt `Selection [1 to 9]`, enter `1` to select **Configure Trusted Nodes**, and press **Enter**.

   The Trusted Nodes Configuration Options menu appears.
4. Perform the following steps for each trusted node you want to add to the configuration:
   a. At the prompt `Selection [1 to 6]`, enter `2` to select **Add a new trusted node configuration**, and press **Enter**.
   b. Enter the local IPv4 node address.
   c. At the prompt `Enter trusted node type`, enter `1` to add a single trusted node to the local IPv4 address you entered in Step B, and press **Enter**.
   d. Enter the IPv4 trusted node address, and press **Enter**.
   e. Enter `y` and press **Enter** to confirm your action.
   f. Repeat Steps A through E for each trusted node you want to add to the configuration.
5. At the prompt `Selection [1 to 6]` for the Trusted Nodes Configuration Options menu, enter `5` to select **Return to main menu**, and press **Enter**.

6. Enter `y` and press **Enter** to confirm your action.

   The IPTables Configurations Options menu appears.

   **Note:**

   The list of trusted nodes is not added to the IPTables rules yet. The changes will be committed to the IPTables rules after you complete this procedure.

7. At the prompt `Selection [1 to 9]`, enter `2` to select **Configure Trusted Ports**, and press **Enter**.

   The Trusted Port Configuration Options menu appears.

8. Perform the following steps for each trusted port you want to be enabled on the server:

   a. At the prompt `Selection [1 to 4]`, enter `1` to select **List all trusted port configuration**, and press **Enter**.

      The list of all trusted port configurations is displayed.

   b. At the prompt `Selection [1 to 4]`, enter `2` to select **Modify a trusted port configuration**, and press **Enter**.

   c. At the prompt `Enter ID of trusted port configuration to be modified`, enter the ID of the port you want to modify (from the list of all trusted port configuration), and press **Enter**.

   d. Press **Enter** to confirm your action.

   e. At the prompt `Enter port status`, enter `1` to enable the port or enter `0` to disable the port.

   f. Press **Enter**.

   g. Press **Enter** to confirm your change.

   h. Repeat Steps A through G for each trusted port you want to enable on the server.

9. At the prompt `Selection [1 to 4]` for the Trusted Port Configuration Options menu, enter `3` to select **Return to main menu**, and press **Enter**.

10. Enter `y` and press **Enter** to confirm your action.

    The IPTables Configurations Options menu appears.

    **Note:**

    The list of trusted ports is not added to the IPTables rules yet. The changes will be committed to the IPTables rules after you complete this procedure.

11. At the prompt `Selection [1 to 9]`, enter `3` to select **DSCP Marking**, and press **Enter**.

    The DSCP Marking Configuration Options menu appears.

12. Perform the following steps for each DSCP value you want to configure on the server:

    a. At the prompt `Selection [1 to 4]`, enter `1` to select **Show DSCP marking configuration**, and press **Enter**.

    The DSCP marking configuration is displayed.

    b. At the prompt `Selection [1 to 4]`, enter `2` to select **Modify DSCP values**, and press **Enter**.

    c. At the prompt `Enter ID of the DSCP category to be modified`, enter the ID of the DSCP value you want to modify (displayed in the DSCP marking configuration), and press **Enter**.

    d. Enter the DSCP value and press **Enter**.

    e. Press **Enter** to confirm your change.

    f. Repeat Steps A through E for each DSCP value you want to configure on the server.

13. At the prompt `Selection [1 to 4]` for the DSCP Marking Configuration Options menu, enter `3` to select **Modify DSCP marking status**, and press **Enter**.
14. Enter `1` to enable the DSCP marking status or enter `0` to disable it.
15. Press **Enter**.
16. Press **Enter** to confirm your change.
17. At the prompt `Selection [1 to 5]` for the DSCP Marking Configuration Options menu, enter `4` to select **Return to main menu**, and press **Enter**.
18. Enter `y` and press **Enter** to confirm your action.

    The IPTables Configurations Options menu appears.

    **Note:**

    The DSCP configuration changes are not added to the IPTables rules yet. The changes will be committed to the IPTables rules after you complete this procedure.
19. At the prompt `Selection [1 to 9]`, enter `5` to select **Commit IPTables Rules**, and press **Enter**.
20. At the prompt `Proceed (Y or N)`, enter `y` and press **Enter**.

    The following warning appears:

    ```
    WARNING: Trusted nodes must include those from which the user logs
    into the current server to perform the maintenance tasks. If you
    have not configured these as trusted nodes, you will not be able to
    log in to the server again after the configuration changes are
    committed.
    ```
21. At the prompt `Proceed (Y or N)`, enter `y` and press **Enter**.
22. Restart the Web Conference Server (WCS) network element.

    This is an important step. If you do not restart the WCS, the WCS will not operate correctly and users will not be able to start or join a Web collaboration.

## Verifying the ACL configuration

### Before you begin

You must be able to log onto the server as a user with the System Security Administrator (SSA) role.

### About this task

Use the following procedure to verify the ACL configuration.

**Note:**

You must perform this procedure on all Avaya Aura® Conferencing core servers and Avaya Media Servers.

### Procedure

1. Log onto the server as a user with the SSA role.
2. At the command prompt, enter `iptstatus -n` and press **Enter**.

   The list of trusted nodes is displayed.
3. Verify that the list of trusted nodes contains the trusted nodes that you configured either in the import file or manually.

   **Note:**

   The full list of trusted nodes contains internal ACL trusted nodes as well as external trusted nodes that you configured either in the import file or manually. The list of external trusted nodes is a subset of all ACL rules.
4. Enter `iptstatus -p` and press **Enter**.

   The list of trusted ports is displayed.
5. Verify that the list of trusted ports matches the trusted ports that you configured either in the import file or manually.
6. Enter `iptstatus -d` and press **Enter**.

   The list of DSCP values is displayed.
7. Verify that the list of DSCP values matches the DSCP values that you configured either in the import file or manually.
8. Ensure that all rules according to the external ACL configuration table are configured. See Access Control List external configuration on page 609.

## Access Control List external configuration

The following table describes how to configure trusted ports, trusted nodes, and DSCP markings on each Avaya Aura® Conferencing server for different deployment layouts.

| Deployment layout | Server | Trusted port | Trusted node | DSCP marking |
|---|---|---|---|---|
| Small to Medium: simplex and redundant | Element Manager | 443<br>8140<br>8141<br>8142<br>6000 to 42599 | • DNS<br>• Remote NTP servers<br>• Remote syslog server<br>• Administrator computer | Disabled |
| Medium: simplex and redundant | Element Manager | 443<br>8140<br>8141<br>8142 | • DNS<br>• Remote NTP servers<br>• Remote syslog server<br>• Administrator computer | Disabled |
| | Avaya Aura® Media Server | 6000 to 42599 | • DNS<br>• Remote NTP servers<br>• Remote syslog server<br>• Administrator computer | Disabled |
| Large: simplex and redundant | Element Manager | 443<br>8140<br>8141<br>8142 | • DNS<br>• Remote NTP servers<br>• Remote syslog server<br>• Administrator computer | Disabled |
| | Web Conferencing Server<br>Avaya Aura® Media Server | 443<br>8140<br>8141<br>8142<br>6000 to 42599 | • DNS<br>• Remote NTP servers<br>• Remote syslog server<br>• Administrator computer | Disabled |
| | Avaya Aura® Media Server | 6000 to 42599 | — | Disabled |

## Example of import.dat

The rules for an external Access Control List (ACL) configuration file are at `/opt/mcp/ipt/example/import.dat`. Follow the instructions in the example file to configure an ACL file.

The following example of the `import.dat` configuration file applies to Element Manager servers in Small to Medium and Medium layouts:

```
trusted node 192.168.209.241 192.168.209.22
trusted node 192.168.209.241 192.168.209.10
trusted node 192.168.209.241 192.168.209.20
trusted node 192.168.209.241 192.168.209.13
siptcpport 5060 0
siptcptlsport 5061 1
httpport 80 1
```

```
httpsport 443 1
wcshttp 8140 0
wcshttps 8141 0
wcsflashpolicy 8142 0
dscpenabled false
dscpvalue   1   48
dscpvalue   2   18
dscpvalue   3   16
mediaports 6000 42599 1
```

# Configuring a file system baseline

### About this task

A baseline is a snapshot of all the system files including their size and permissions. You can compare baselines from various times to determine what has changed over a given period of time. You should create baselines on a regular basis or if there are any significant changes to the system, such as an upgrade.

This task must be performed on all Element Manager servers and Avaya media servers.

### Procedure

1. Log onto the server using the System Security Administrator (SSA) username.
2. At the command prompt, enter **`fsibaseline`** and press **Enter**.

   At any time, you can compare the current system against previous baselines to determine what has changed. Refer to the Security Guide for more details on managing and comparing baselines.

# Enabling Tomcat webserver access and error logs for the Element Manager

### Procedure

1. Open the browser and access Element Manager Console from System Manager.
2. In the navigation pane of Element Manager Console, click **Feature Server Elements > Element Manager > Element Manager > Configuration Parameters**.
3. From the **Parm Group** drop-down box in the Element Manager Configuration Parameters window, select **WebServer**.
4. Select **EnableAccessLogs**.
5. Click **Edit (-/+)**.
6. From the Value box, select **true**.
7. Click **Apply**.

8. Close the Element Manager Configuration Parameters window.

## Enabling Tomcat webserver access logs and audit logging for the Provisioning Manager

### About this task

Use this task to enable the following settings for all Provisioning Managers in the system:

- Tomcat webserver access and error logs
- the generation of audit logs for Collaboration Agent and SOPI requests

### Procedure

1. Open the browser and access Element Manager Console from System Manager.
2. In the navigation pane of Element Manager Console, click **Feature Server Elements > Provisioning Managers > <*Provisioning Manager name*> > Configuration Parameters**.
3. From the **Parm Group** drop-down box in the Provisioning Manager Configuration Parameters window, select **WebServer**.
4. Select **EnableAccessLogs**.
5. Click **Edit (-/+)**.
6. From the Value box, select **true**.
7. Click **Apply**.
8. From the **Parm Group** drop-down box in the Provisioning Manager Configuration Parameters window, select **PersonalAgent**.
9. Select **GenerateAuditLogs**.
10. Click **Edit (-/+)**.
11. From the Value box, select **true**.
12. Click **Apply**.
13. Close the Provisioning Manager Configuration Parameters window.
14. Repeat Steps 2 through 14 for each Provisioning Manager.

# Enabling Tomcat webserver access logs and audit logging for the Collaboration Agent Manager

### About this task

Use this task to enable the following settings for all Collaboration Agent Managers in the system:

- Tomcat webserver access and error logs
- the generation of audit logs for Collaboration Agent and SOPI requests

### Procedure

1. Open the browser and access Element Manager Console from System Manager.
2. In the navigation pane of Element Manager Console, click **Feature Server Elements > Collaboration Agent Managers > <*Collaboration Agent Manager name*> > Configuration Parameters**.
3. From the **Parm Group** drop-down box in the Collaboration Agent Manager Configuration Parameters window, select **WebServer**.
4. Select **EnableAccessLogs**.
5. Click **Edit (-/+)**.
6. From the Value box, select **true**.
7. Click **Apply**.
8. From the **Parm Group** drop-down box in the Collaboration Agent Manager Configuration Parameters window, select **CollaborationAgent**.
9. Select **GenerateAuditLogs**.
10. Click **Edit (-/+)**.
11. From the Value box, select **true**.
12. Click **Apply**.
13. Close the Collaboration Agent Manager Configuration Parameters window.
14. Repeat Steps 2 through 14 for each Collaboration Agent Manager.

# Configuring local logon password policies for Element Manager Console and Provisioning Client

### About this task

Use this procedure to configure the password policies for the local logon administration accounts for Element Manager Console and Provisioning Client.

**Note:**

The local logon account password policies do not affect the single-sign on (SSO) passwords used to access Element Manager Console and Provisioning Client via System Manager.

### Procedure

1. Open the browser and access Element Manager Console locally`https://`*`<FQDN>`*`:12121`.

   where *<FQDN>* is the EM Internal OAM Service Fully Qualified Domain Name (FQDN). This is the FQDN of the EM Internal OAM Service IP address.

2. Log in as the *admin* user.
3. From the Administration menu in Element Manager Console, select **Password Rules**.
4. In the Password Rules dialog box, update each setting according to the values in **EM/Prov Admin Password Policy** section of the Avaya Aura® Conferencing Intelligent Workbook.
5. When finished, click **Apply**.

## Configuring local logon account login rules for Element Manager Console and Provisioning Client

### About this task

Use this procedure to configure the login rules for the local logon administration accounts for Element Manager Console and Provisioning Client.

**Note:**

The local logon login rules do not affect the single-sign on (SSO) logon accounts used to access Element Manager Console and Provisioning Client via System Manager.

### Procedure

1. Open the browser and access Element Manager Console locally`https://`*`<FQDN>`*`:12121`.

   where *<FQDN>* is the EM Internal OAM Service Fully Qualified Domain Name (FQDN). This is the FQDN of the EM Internal OAM Service IP address.

2. Log in as the *admin* user.
3. From the Administration menu in Element Manager Console, select **Login Rules**.
4. From the **Login Interface** drop-down box in the Login Rules dialog box, select **Configuration Management (OMI)**.
5. Update each setting for the Element Manager Console local logon accounts according to the values in **OMI - Session Timeout (minutes), OMI - Failed Login Attempts before**

**Lockout, OMI - Lockout Duration (minutes)** and **OMI - Account Inactivity (days)** in the Avaya Aura® Conferencing Intelligent Workbook.

6. From the **Login Interface** drop-down box, select **Provisioning Management (PROV)**.
7. Update each setting for the Provisioning Client local logon accounts according to the values in **Prov - Session Timeout (minutes), Prov - Failed Login Attempts before Logout, Prov - Lockout Duration (minutes)** and **PROV - Account Inactivity (days)** in the Avaya Aura® Conferencing Intelligent Workbook.
8. Click **Apply**.

# Changing the Element Manager SNMP community string

## About this task

The SNMP community string can only be changed for servers that are online and reachable on the network. Before performing this task, ensure that all servers in the system are reachable from the active Element Manager's server.

## Procedure

1. Open the browser and access Element Manager Console from System Manager.
2. In the navigation pane of Element Manager Console, click **Feature Server Elements > SNMP Profiles**.
3. In the SNMP Profiles window, click **Add (+)**.
4. In the Add Server SNMP Profiles dialog box, perform the following steps:
    a. In the Profile Name box, enter the appropriate SNMP profile name.
    b. In the Read Community String box, enter the appropriate SNMP Read Community String.
    c. In the Write Community String box, enter the appropriate SNMP Write Community String.
    d. Click **Apply**.
5. Close the SNMP Profiles window.
6. In the navigation pane of Element Manager Console, click **Servers**.
7. In the Servers window, select the server.
8. Click **Edit (-/+)**.
9. From the SNMP Profile drop-down box in the Edit Server dialog box, select the appropriate SNMP profile name.
10. Click **Apply**.
11. Repeats Steps 8 through 11 for each server listed.

**Note:**

If new servers are added, be sure to select the new SNMP profile when creating the new server.

# Removing the default staging certificates

## About this task

The final step in hardening the system is to remove the default staging certificates from the truststore. Make sure *all* sanity checks (including talking to the Avaya media server) have been successfully completed before performing this task. Once this task is completed, the system will no longer be accessible via the staging certificate.

**Note:**

You must restart the network elements after performing this procedure.

## Procedure

1. Open the browser and access Element Manager Console from System Manager.
2. In the navigation pane of Element Manager Console, click **Security > Certificate Management > Truststore**.
3. In the Truststore window, select the row that contains **CN=Default Staging Certificate**.
4. Click **Delete (-)**.
5. In the Confirmation dialog box, click **Yes**.
6. Restart the network elements for the changes to take effect and to clear alarms.

# Configuring Avaya Media Server DSCP

## About this task

This task must be performed for each Avaya Media Server cluster in the system.

## Procedure

1. Open the browser and access Element Manager Console from System Manager.
2. In the navigation pane of Element Manager Console, click **Feature Server Elements > Media Servers and Clusters > Media Server Clusters > <*Cluster name*> > DSCP Settings**.
3. In the **SIP QoS DSCP** box in the DSCP Settings dialog box, enter the appropriate value.
4. In the **Audio QoS** box, enter the appropriate value.

5. In the **Video QoS** box, enter the appropriate value.
6. Click **Apply**.
7. Restart the Avaya Media Server network elements for the cluster.
8. Repeat Steps 2 through 7 for each Avaya Media Server cluster in the system.

# Fixing remote host SSH keys

## About this task

When an SSH session is created for the first time, the remote servers public key is stored in `/root/.ssh/known_hosts`. If this key changes for any reason (a server reinstall is the primary reason), then SSH will not allow a connection to continue until that key is manually removed from the `known_hosts` file.

If the following warning is displayed when running the mcpInstIntACLConf scripts, the file `/root/.ssh/known_hosts` must be modified before the SSH connection to the remote server will succeed:

```
WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! IT IS POSSIBLE THAT
SOMEONE IS DOING SOMETHING NASTY! Someone could be eavesdropping on you
right now (man-in-the-middle attack)! It is also possible that the RSA
host key has just been changed. The fingerprint for the RSA key sent by
the remote host is 60:75:7a:9e:af:88:85:e7:c7:3d:82:d6:c5:7e:a8:a8.
Please contact your system administrator. Add correct host key in /
root/.ssh/known_hosts to get rid of this message.
```

To modify the file `/root/.ssh/known_hosts`, perform this task on the server where the script is being run.

## Procedure

1. Log onto the server as an SSA user.
2. At the command prompt, enter **`su -`** and press **Enter**.
3. Enter the root password and press **Enter**.
4. Edit the file `/root/.ssh/known_hosts`.

   Each line in this file has an IP address followed by the public key for that IP address.
5. Delete the line for the remote server.
6. Save the file.
7. Once the file has been modified, retry the script from the same server.

# Chapter 36: Configuring collaboration aware clients for Avaya Aura® Conferencing

This chapter describes the settings you must configure to use the following “collaboration aware” clients with Avaya Aura® Conferencing:

- Avaya Equinox for Windows
- Avaya Equinox for iOS
- the following Avaya 96x1 SIP telephones:
    - Avaya 9608 SIP Telephone
    - Avaya 9611G SIP Telephone
    - Avaya 9621G SIP Telephone
    - Avaya 9641G SIP Telephone

**Related links**

Configuring the settings for Avaya Equinox for Windows on page 618
Configuring the settings for Avaya Equinox for iOS on page 619
Configuring the settings for Avaya 96x1 SIP telephones on page 620

## Configuring the settings for Avaya Equinox for Windows

### About this task

Use this procedure to configure the appropriate settings in Avaya Communication Manager and System Manager for Avaya Equinox for Windows.

Use the Avaya Aura® System Manager administration interface to modify the Avaya Communication Manager settings and add or modify a user. For more information, see *Installing and Configuring Avaya Aura® Session Manager* on the Avaya Web site at http://www.avaya.com/support.

**Note:**

Avaya Equinox for Windows supports only SIP endpoints. H.323 endpoints are not supported.

**Note:**

In order to view screen sharing in the Avaya Equinox® Client, users must have a Conferencing profile in Avaya Aura Conferencing.

### Procedure

1. For Avaya Communication Manager, perform the following steps:
   - For the Communication Manager signaling group associated with Avaya Session Manager, set **Initial IP-IP Direct Media** to **y**.
   - On page 19 of System Parameters – Features, set **SIP Endpoint Managed Transfer** to **y**.
   - On page 4 of the IP-Options System Parameters, set **Override ip-codec-set for SIP direct-media connections** to **y**.
2. For each Avaya Equinox for Windows extension, perform the following steps:
   - Set an **Avaya E.164** communication address.
   - Set Template to 9640SIP (for example, **DEFAULT_9640SIP_CM_6_2**).
   - Enable **IP SoftPhone**.
   - Enable **IP Video Softphone**.
   - Set **Type of 3PCC Enabled** to **Avaya**.
   - Configure eight call appearances to provide support for Adhoc conferences.
   - Enable **Presence Buddy** for Aura® contacts.
   - Set **Origination Application Sequence** to the Communication Manager server.
   - Set **Termination Application Sequence** to the Communication Manager server.
   - Enable **Conference Profile** and configure the settings for the user's Avaya Aura® Conferencing profile.

**Related links**

Configuring collaboration aware clients for Avaya Aura Conferencing on page 618

## Configuring the settings for Avaya Equinox for iOS

### About this task

Use this procedure to configure the appropriate settings in Avaya Communication Manager and System Manager for Avaya Equinox for iOS.

Use the Avaya Aura® System Manager administration interface to modify the Avaya Communication Manager settings and add or modify a user. For more information, see *Installing and Configuring Avaya Aura® Session Manager* on the Avaya Web site at http://www.avaya.com/support.

**Note:**

Avaya Equinox for iOS supports only SIP endpoints. H.323 endpoints are not supported.

### Procedure

1. For Avaya Communication Manager, perform the following steps:
   - For the Communication Manager signaling group associated with Avaya Session Manager, set **Initial IP-IP Direct Media** to **y**.
   - On page 19 of System Parameters – Features, set **SIP Endpoint Managed Transfer** to **y**.
   - On page 4 of the IP-Options System Parameters, set **Override ip-codec-set for SIP direct-media connections** to **y**.
2. For each Avaya Equinox for iOS extension, perform the following steps:
   - Set an **Avaya E.164** communication address.
   - Set Template to 9640SIP (for example, **DEFAULT_9640SIP_CM_6_2**).
   - Enable **IP SoftPhone**.
   - Set **Type of 3PCC Enabled** to **Avaya**.
   - Configure eight call appearances to provide support for Adhoc conferences.
   - Enable **Presence Buddy** for Aura® contacts.
   - Set **Origination Application Sequence** to the Communication Manager server.
   - Set **Termination Application Sequence** to the Communication Manager server.
   - Enable **Conference Profile** and configure the settings for the user's Avaya Aura® Conferencing profile.

#### Related links

Configuring collaboration aware clients for Avaya Aura Conferencing on page 618

## Configuring the settings for Avaya 96x1 SIP telephones

### About this task

Use this procedure to configure the appropriate settings in the 46xxsettings.txt file and System Manager for the following Avaya 96x1 SIP telephones:

- Avaya 9608 SIP Telephone
- Avaya 9611G SIP Telephone
- Avaya 9621G SIP Telephone
- Avaya 9641G SIP Telephone

Use the Avaya Aura® System Manager administration interface to add or modify a user. For more information, see *Installing and Configuring Avaya Aura® Session Manager* on the Avaya Web site at http://www.avaya.com/support.

### Procedure

1. In the 46xxsettings.txt file, set the parameter `CONFERENCE_FACTORY_URI` to the Adhoc conferencing service URI access number with SIP domain. For example, if the Adhoc conferencing service URI access number with SIP domain is 1244501@yourcompany.com, you would specify the following text in the 46xxsettings.txt file:`SET CONFERENCE_FACTORY_URI “1244501@yourcompany.com”`)
2. For each Avaya 96x1 SIP telephone extension, perform the following steps:
   - Configure eight call appearances to provide support for Adhoc conferences.
   - Enable **Conference Profile** and configure the settings for the user's Avaya Aura® Conferencing profile.

**Related links**

Configuring collaboration aware clients for Avaya Aura Conferencing on page 618

# Chapter 37: Deploying the Avaya Aura® Conference Manager Add-in for Microsoft Outlook®

Conference Manager for Microsoft Outlook supports Microsoft Outlook 2007, Microsoft Outlook 2010, Microsoft Outlook 2013, and Microsoft Outlook 2016. Conference Manager for Microsoft Outlook does not support installation with the Avaya Client Applications Collaboration Services plug-in for Microsoft Outlook. These plug-ins provide the same conferencing functions and conflict with each other.

For more information, see *Avaya Client Applications Collaboration Services User Guide*.

The Avaya Aura® Conference Manager Add-in for Microsoft Outlook® uses Outlook's Calendar Meeting feature to help users create and manage their conference invitations. The Avaya Aura® Conference Manager Add-in for Microsoft Outlook® conference invitations display the conferencing telephone numbers that you have configured as the Service URI, or if you have configured display telephone numbers, Avaya Aura® Conference Manager Add-in for Microsoft Outlook® displays the display telephone numbers.

You can use one of the following models for deploying the Avaya Aura® Conference Manager Add-in for Microsoft Outlook®:

- ClickOnce deployment

  With the ClickOnce deployment, you must place the Avaya Aura® Conference Manager Add-in files on to a web server or other public location (like a network share) that Avaya Aura® Conferencing users can access. The users will then run the Avaya Aura® Conference Manager Add-in installer from that location. Once the users install the Avaya Aura® Conference Manager Add-in, updates will be applied automatically when available. For this deployment, each user must run the installer.

- Centralized software deployment

  With the centralized software deployment, you may configure a group policy so that individual computer configurations are updated. The Windows registry is modified to point to the Microsoft Outlook Add-in deployment manifest. When Microsoft Outlook is restarted, it will automatically download the Avaya Aura® Conference Manager Add-in from the specified location.

**Note:**

Once installed, the Avaya Aura® Conference Manager Add-in will check for updates every two weeks at the same location from which Avaya Aura® Conference Manager Add-in was installed. Make sure that location contains the latest version of the Avaya Aura® Conference Manager Add-in. To publish an updated version of the Avaya Aura® Conference Manager Add-in, remove the contents of the folder at that location, and then place the new files in that location.

**Related links**

Implementing a ClickOnce deployment on page 623
Implementing a centralized software deployment on page 625
Configuring a Web conferencing host on page 226
Configuring display numbers in Provisioning Client on page 317
Adding conference access numbers in Provisioning Client on page 313

## Implementing a ClickOnce deployment

### Before you begin

- You must have the file *asu_version_date_time.zip* (for example, *asu_1.0.0.176_2012-12-13_15-44-20.zip*) , which is bundled with Collaboration Agent. The file *asu_version_date_time.zip* is located in `/var/mcp/media/prov_pa_installs/outlook/asu` on the server where Avaya Aura® Conferencing is installed.
- To use the Avaya Aura® Conference Manager Add-in for Microsoft Outlook®, a user must have:
  - Microsoft Outlook 2007/2010/2013/2016 installed
  - an account (with a moderator code) on the Avaya Aura® Conferencing system

### About this task

Use this procedure to implement the Avaya Aura® Conference Manager Add-in for Microsoft Outlook using the ClickOnce deployment. With the ClickOnce deployment, each user must run the Avaya Aura® Conference Manager Add-in installer.

### Procedure

1. Unzip the contents of the file *asu_version_date_time.zip* (for example, *asu_1.0.0.176_2012-12-13_15-44-20.zip*) on a web server that all users can access. The file *asu_version_date_time.zip* contains the installation files for the Avaya Aura® Conference Manager Add-in. The file *asu_version_date_time.zip* is located in `/var/mcp/media/prov_pa_installs/outlook/asu` on the server where Avaya Aura® Conferencing is installed.
2. Open your web browser and make sure you can browse the folder on the web server that contains the files you unzipped in Step 1.
3. From the folder that contains the installation files for the Avaya Aura® Conference Manager Add-in, download the file *setup.exe* to a PC running Microsoft Windows.

4. On the Windows PC that contains the file *setup.exe* that you downloaded in Step 3, perform the following steps:
   a. Select **Start > All Programs > Accessories > Command Prompt**.
   b. In the Command Prompt window, type the following command:

      ```
      setup.exe -url="http://FQDN_or_IP_address_of_your_server/
      Outlook Add-In"
      ```

      where `"http://FQDN_or_IP_address_of_your_server/Outlook Add-In"` is the URL to the folder that contains the Avaya Aura® Conference Manager Add-in installation files.
   c. Upload the modified *setup.exe* file back to the folder that contains the installation files for the Avaya Aura® Conference Manager Add-in.
5. Make sure each user performs the following steps to install the Avaya Aura® Conference Manager Add-in:
   a. Open your web browser and go to the folder that contains the Avaya Aura® Conference Manager Add-in installation files.
   b. Click **setup.exe**.
   c. When prompted to run or save setup.exe, click **Run**.
   d. When prompted to confirm that you want to run this program, click **Run**.
   e. In the Avaya Aura Conference Manager Setup dialog box, read the license agreement.
   f. Click **Accept** to accept the terms of the license agreement.
   g. In the Microsoft Office Customization Installer dialog box, click **Install**.

      The Avaya Aura® Conference Manager Add-in is installed.
   h. When the installation is complete, click **Close**.
   i. Start Microsoft Outlook.

      The Avaya Aura dialog box should appear, prompting you to enter your user name, password, and service host.

      The service host is the name of the Web Conferencing Host that you entered in the Provisioning Client window. It must be the hostname, not the IP address.
   j. Enter your user name, password, and address of the service host, and then click **Save**.

**Related links**

Deploying the Avaya Aura Conference Manager Add-in for Microsoft Outlook on page 622
Configuring a Web conferencing host on page 226

# Implementing a centralized software deployment

### Before you begin

- To use the Avaya Aura® Conference Manager Add-in, the PC must contain the following software:
  - Microsoft Outlook 2007/2010/2013/2016 installed
  - Microsoft Windows Installer 3.1. (Typically, this is already present on a Windows PC.)
  - Microsoft .NET 4.0 Framework Client Profile
  - Microsoft VSTO 4.0 Runtime
  - Avaya Event Log Source. This software configures the source in the Windows System Event Log so that the Microsoft Outlook Add-in can log events under the name **Avaya Aura Outlook Conference Manager**.

  Microsoft Windows Installer 3.1, Microsoft .NET 4.0 Framework Client Profile, Microsoft VSTO 4.0 Runtime, and Avaya Event Log Source are available in the file *asu_version_date_time.zip* (for example, *asu_1.0.0.176_2012-12-13_15-44-20.zip*), which is bundled with Collaboration Agent. The file *asu_version_date_time.zip* is located in `/var/mcp/media/prov_pa_installs/outlook/asu` on the server where Avaya Aura® Conferencing is installed.
- You have Administrative privileges on the Windows PC. (You need to access the Windows Registry.)

### About this task

Use this procedure to implement the Avaya Aura® Conference Manager Add-in for Microsoft Outlook using the centralized deployment. With the centralized deployment, you can configure your domain to remotely deploy software to client computers from a central location.

### Procedure

1. Unzip the contents of the file *asu_version_date_time.zip* (for example, *asu_1.0.0.176_2012-12-13_15-44-20.zip*) to a folder. The file *asu_version_date_time.zip* contains the installation files for the Microsoft Outlook Add-in. The file *asu_version_date_time.zip* is located in `/var/mcp/media/prov_pa_installs/outlook/asu` on the server where Avaya Aura® Conferencing is installed.
2. Modify the Windows Registry file *aacAddin.reg* to point to the location of the deployment manifest for the Avaya Aura® Conference Manager Add-in. An example of the manifest setting in the Windows Registry is:

   ```
   “Manifest”=”http://localhost/Outlook Add-In v.1.0.0.141/
   Avaya.Aura.ConferenceManager.vsto”
   ```
3. On each client PC, perform the following steps:
   a. Install Microsoft VSTO 4.0 Runtime.
   b. Install Avaya Event Log Source.
   c. Install Microsoft .NET 4.0 Framework Client Profile.

d. Download and save the file *aacAddin.reg* to your desktop.

e. Right-click on *aacAddin.reg* and select **Merge**.

f. Exit Microsoft Outlook.

g. Restart Microsoft Outlook.

h. In the Microsoft Office Customization Installer dialog box, click **Install**.

   The Avaya Aura dialog box should appear, prompting you to enter your user name, password, and service host.

   The service host is the name of the Web Conferencing Host that you entered in the Provisioning Client window. It must be the hostname, not the IP address.

i. Enter your user name, password, and address of the service host, and then click **Save**.

**Related links**

Deploying the Avaya Aura Conference Manager Add-in for Microsoft Outlook on page 622
Configuring a Web conferencing host on page 226

# Chapter 38: Uninstalling software

## Introduction to uninstalling software

The mcpInstaller script is used for new Avaya Aura® Conferencing installations only. If you need to reinstall or upgrade, use the procedures in this chapter to undeploy and uninstall current applications prior to running the mcpInstaller script.

**Important:**

After you have uninstalled the current applications, start the mcpInstaller script and select no at the prompt to resume from a previous installation. You must start from the beginning of the script.

## Checklist for uninstalling Application Server software

The following checklist provides the workflow for uninstalling the Application Server software.

**Table 40: Workflow for uninstalling the Application Server software**

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Stop and undeploy all network element instances except for Element Manager instances. | See Stopping and undeploying a network element instance on page 628. | | |
| 2 | Undeploy Element Manager. | See Stopping and undeploying Element Manager on page 628. | | |
| 3 | Cleanup the Application Server database or Uninstall the Application Server. | See Cleaning up the Application Server database on page 628 or Uninstalling the database software on page 629 if a reinstallation is required. | | |

# Stopping and undeploying a network element instance

### About this task

Stop and undeploy a network element instance.

### Procedure

1. In the navigation pane of the Element Manager Console, click **Feature Server Elements**, and select the <NE Type> and <NE> for the instance you want to stop. For example, to stop a Media Server network element instance, click **Media Servers and Clusters** > **Media Servers** and select the <Media Server NE> for the instance you want to stop.
2. Click **NE Maintenance**.
3. In the Maintenance dialog box, select the row for ID 0, and click **Stop**.
4. In the Maintenance dialog box, select the row for ID 1 (if it exists), and click **Stop**.
5. After the stop operation completes, select the row for ID 0, and click **Undeploy**.
6. Select the row for ID 1 (if it exists), and click **Undeploy**.

# Stopping and undeploying Element Manager

### Before you begin

If you have a secondary Element Manager, you must stop and undeploy from the Element Manager console.

### About this task

Stop and undeploy the primary Element Manager.

### Procedure

1. Log on to EMServer0 as `ntappadm` through ssh or directly at the server console.
2. Type `emUndeploy.pl`, and press **Enter**.
3. Type **y** to all prompts, and press **Enter**.

### Result

The Element Manager instance 0 is now stopped and uninstalled.

# Cleaning up the Application Server database

### Before you begin

All Network Element instances must be stopped.

### About this task

Cleanup the Application Server database.

### Procedure

1. Log on to EMServer0 as ntappadm through ssh.
2. Type `dbUninstall.pl`, and press **Enter**.
3. Type `y` to all prompts, and press **Enter**.

### Result

The Application Server database has been cleaned.

## Uninstalling the database software

Uninstalling the database software is not usually necessary. A clean up of the database is generally sufficient.

### Before you begin

Stop and undeploy all network element instances.

### About this task

Use this procedure to uninstall the database software if a complete reinstallation of the software is required.

### Procedure

1. Log on to EMServer0 as `ntappadm` through ssh.
2. Type `cd /var/mcp/install`, and press **Enter**.
3. Type `./mcpDbSwUninstall.pl –primary`, and press **Enter**.
4. Type `y` to all prompts, and press **Enter**.
5. For redundant deployments (non-simplex), type `./mcpDbSwUninstall.pl –secondary`, and press **Enter**.
6. Type `y` to all prompts, and press **Enter**.

### Result

The application database software is uninstalled.

# Checklist for uninstalling the Avaya Aura® Media Server software

The following checklist provide the workflow for uninstalling the Avaya Aura® Media Server software.

**Table 41: Workflow for uninstalling the Avaya Aura® Media Server software**

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Stop and undeploy the Media Server instances. | See Stopping a network element instance on page 659 and Undeploying a network element instance on page 659. | | |
| 2 | Uninstall the Media Server software. | See Uninstalling the Avaya Media Server on page 630. | | |

# Uninstalling the Avaya Aura® Media Server

If your deployment has existing recording files, Avaya recommends backing up the recording files. The uninstall script, mcpMsUnintall.pl, displays a prompt to provide you with the option of backing up then restoring the recording files.

## Before you begin

Stop and undeploy the Media Server network elements.

## About this task

Uninstall the Avaya Aura® Media Server software.

## Procedure

1. Log on to `ntsysadm` through ssh or directly at the server console.
2. Enter **`su -`** to log on as root.
3. Type `mcpMsUninstall.pl`, and press **Enter**.
4. At the prompt to `Continue uninstall?`, type `y`, and press **Enter**.

   The following message is displayed:

   ```
   If your lab has recording data that you want to preserve - it is recommended for
   you to
   backup Media Server configuration.
   ```

5. **(Optional)** At the **Do you want to preserve Recordings data on local drive (Y/N)?** prompt, type `y` and press **Enter**.

The following message is displayed:

```
In order to continue using recordings data on local drive you will also need to
restore
Media Server configuration.
If you have already backed up Media Server configuration you can skip this step
```

6. **(Optional)** At the **Do you want to backup Media Server configuration (Y/N)?** prompt, type `y` and press **Enter**.

   The uninstaller executes the uninstall scripts.

### Result

The message `Uninstall completed SUCCESSFULLY` appears. The Avaya Aura® Media Server software is now uninstalled.

# Appendix A: Shutting down and starting the Avaya Aura® Conferencing system

## Shutting down the Avaya Aura® Conferencing system

### About this task

Use the following procedure to shut down the Avaya Aura® Conferencing system.

### Procedure

1. Log on to the Element Manager Console using an account with admin privileges.
2. Stop all network element instances except for the primary Element Manager instance (EM_0).

   For more information about stopping network elements, see Stopping and undeploying a network element instance on page 628.
3. Log on to the EM_0 server as ntappadm to stop the primary network element instance for EM_0.
   1. Type `cd /var/mcp/install`, and press **Enter**.
   2. Type `./emStop.pl`.
4. Log on to the primary database server as `ntsysadm` or an account with the SSA role through ssh or directly on the server console to stop the database and replication.
   1. Type `stopRep`, and press **Enter**.
   2. If prompted, type the password for the SSA account.
   3. Type `stopDB`, and press **Enter**.
5. Power off the server.

# Starting the Avaya Aura® Conferencing system after a shutdown

### Before you begin

The servers must be powered up.

### About this task

Use the following procedure to start the Avaya Aura® Conferencing system after a shutdown.

**Note:**

To determine the current status of the database, on the command line, log on as `ntsysadm`, and type `statusOfDB`.

### Procedure

1. If the secondary database was stopped, log on to the secondary database server (EMServer2), as `ntsysadm` or an account with the SSA role through ssh or directly on the server console.

   Type `startDB` to start the database, and press **Enter**.

2. If the primary database was stopped, log on to the primary database server (EMServer1), as `ntsysadm` or an account with the SSA role through ssh or directly on the server console.

   a. Type `startDB` to start the database, and press **Enter**.

   b. Type `startRep` to start replication, and press **Enter**.

3. Log on to the primary Element Manager (EMServer1) hosting Element Manager instance 0 (EM_0) as `ntappadm` or an account with the AA role through ssh or directly on the server console.

   a. Type `cd /var/mcp/install`, and press **Enter**.

   b. Type `./emStart.pl`, and press **Enter**.

4. From the Element Manager Console, start all network element instances.

   For more information about starting network elements, see the chapter for Deploying and starting the remaining Network Elements.

# Appendix B: Migrating existing data to the new Avaya Aura Conferencing release

## Introduction to migrating your data

Avaya has created a migration tool for migrating your data from older conferencing solutions to the latest Avaya Aura® Conferencing release. The migration tool imports the user data and the on-demand conference data. The migration tool does not import the scheduled conference data. The latest version of the migration tool is version 3.0. This version of the tool enables you to migrate your data directly to either of the Avaya Aura® Conferencing deployment configurations. So, the migration tool operates successfully if you have an Avaya Aura® environment or a Turnkey environment[13]. You should use version 3.0 of the migration tool to migrate your data from any of the following applications:

- Meeting Exchange 5.2 or 6.2
- Avaya Aura® Conferencing 6.0

It is important to note that version 3 of the tool is not compatible with Avaya Aura® Conferencing 7.2. To migrate your data from Avaya Aura® Conferencing 7.2, use the upgrade process instead.

**Note:**

A separate WebLM server is required if you want to maintain your current Meeting Exchange or Avaya Aura® Conferencing license while adding a new Avaya Aura® Conferencing license for the new release.

**Related links**

Implementation on page 21

[13] You can deploy Avaya Aura® Conferencing with the Avaya Aura® platform. The Avaya Aura® platform consists of Avaya Aura® System Manager, Avaya Aura® Session Manager, and Avaya Aura® System Platform. This type of deployment is called an Avaya Aura® deployment. Alternatively, you can deploy Avaya Aura® Conferencing without the Avaya Aura® platform. This type of deployment is called a Turnkey deployment.

# Checklist of migration tasks

If you have an Avaya Aura® deployment, complete the tasks in Checklist of migration tasks on page 635. In an Avaya Aura® deployment, you must import the conference users into System Manager and you must import the conference types and conference templates directly into the Avaya Aura® Conferencing Provisioning Manager. System Manager then forwards the user data to Avaya Aura® Conferencing.

**Table 42: Avaya Aura®**

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Install the tool. | Installing the data migration tool on page 636 | | |
| 2 | Export the data from the old system. | Exporting data from Meeting Exchange or older versions of Avaya Aura Conferencing on page 637 | | |
| 3 | Test the connection between Avaya Aura® Conferencing and System Manager. | Checking the connection between Avaya Aura Conferencing and System Manager on page 638 | | |
| 4 | Import the data in to the Avaya Aura® Conferencing for Avaya Aura® system. | Importing data to Avaya Aura Conferencing for Avaya Aura on page 638 | | |

If you have a Turnkey deployment, complete the tasks in Table 43: Turnkey on page 635. In a Turnkey deployment, you must import the conference types, conference templates, and the conference users directly into the Avaya Aura® Conferencing Provisioning Manager.

**Table 43: Turnkey**

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Install the tool. | Installing the data migration tool on page 636 | | |
| 2 | Export the data from the old system. | Exporting data from Meeting Exchange or older versions of Avaya Aura Conferencing on page 637 | | |

*Table continues…*

| No. | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 3 | Import the data in to the Avaya Aura[®] Conferencing for Turnkey system. | Importing data to Avaya Aura Conferencing for Turnkey on page 644 | | |

# Installing the data migration tool

The data migration tool is a Windows desktop application that runs under Windows XP or the Windows 7 or 8 Operating Systems.

## Before you begin

- Windows XP, 7, or 8 operating system is installed.
- The minimum hardware requirements are met.
- Microsoft .NET Framework 4 Client Profile is installed on the target server.

## About this task

Use the following procedure to install the data migration tool to your computer.

## Procedure

1. Download the AAC Data Migration Tool software from Avaya PLDS.

   Ensure that the tool is version 3.0.9 or later.
2. Double-click the **AAC Data Migration Tool msi** to start the installation.

   **Note:**

   If an older version of the installer already exists, you must remove it before continuing.
3. At the Welcome to the Avaya AAC Data Migration Tool Setup Wizard screen, click **Next**.
4. At the Select Installation Folder screen, click **Browse** to install the software to another folder.
5. Click **Just me** to ensure that the Data Migration Tool can only be used by you on this computer or click **Everyone** to allow anyone who uses this computer to use this tool.
6. Click **Next** to continue or to accept the default folder location.
7. At the Confirm Installation screen, click **Next.**

   After the installation completes, you see the message **Avaya AAC Data Migration Tool has been successfully installed**.
8. Click **Close**.

### Next steps

Proceed to Exporting data from Meeting Exchange or older versions of Avaya Aura Conferencing on page 637.

**Related links**

Prerequisites for software installation on page 119

## Exporting data from Meeting Exchange or older versions of Avaya Aura® Conferencing

### Before you begin

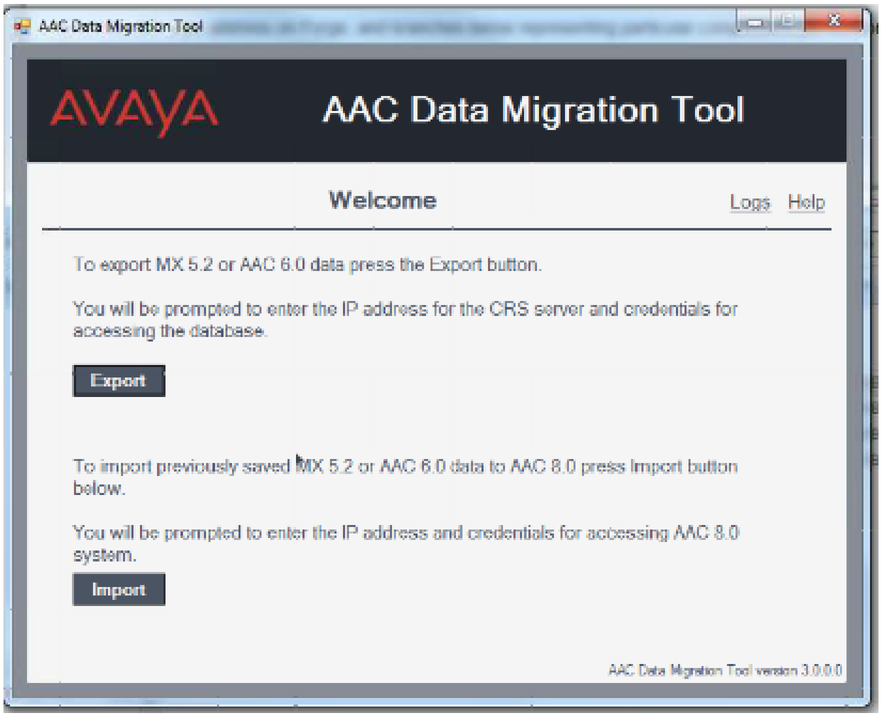
- Obtain the SQL Server Database credentials for your Meeting Exchange system.
- Obtain the user name and password for the older Avaya Aura® Conferencing system.

### About this task

Use the following procedure to export your existing data from Meeting Exchange or older versions of Avaya Aura® Conferencing to the new Avaya Aura® Conferencing release.

### Procedure

1. In the Welcome window, click **Export**.



To export MX 5.2 or AAC 6.0 data press the Export button.

You will be prompted to enter the IP address for the CRS server and credentials for accessing the database.

To import previously saved MX 5.2 or AAC 6.0 data to AAC 8.0 press Import button below.

You will be prompted to enter the IP address and credentials for accessing AAC 8.0 system.

AAC Data Migration Tool version 3.0.0.0

**Figure 31: Welcome screen**

2. In the Export dialog box, in the CRS server section, complete the following:
   - **Host name or IP address**: Type the hostname or IP address of the SQL server where the CRS database resides.
   - **Database username**: Type **sa**. This is the default username. The username in your deployment may be different.
   - **Database password**: Type the password that you configured during installation.
3. Click **Test Connection** and confirm that the message **Connected OK** is displayed.
4. In the Storage section, click the ellipsis (...) to specify a location to save your data.

   **Note:**

   Your exported data is backed up using the file name mxbackup.xml.
5. Click **Export**.

   When the export is complete, the message **Export finished** is displayed.
6. Click **Back to Main** to return to the main window.

## Checking the connection between Avaya Aura® Conferencing and System Manager

For a successful import of the User information to System Manager, you need to verify that the Avaya Aura® Conferencing server is connected to System Manager. This test requires single-sign-on (SSO). For more information on SSO, see Introduction to SSO on page 304.

## Importing data to Avaya Aura® Conferencing for Avaya Aura®

The import process involves the following:

- Defines a domain which is appended to the qualified username for Avaya Aura® Conferencing, for example, user1@domain.com.
- Defines a user's location, user's timezone, and Session Manager name.
- Imports Meeting Exchange the on-demand conference data and user templates into Avaya Aura® Conferencing profiles. The migration tool does not import the scheduled conference data.
- Prepares an XML file containing user information and imports users to System Manager using the System Manager bulk import process.

## Before you begin

- Export the data from Meeting Exchange or the older version of Avaya Aura® Conferencing.
- Install the latest release of Avaya Aura® Conferencing.
- Check to ensure that Avaya Aura® Conferencing is connected to the System Manager.

For more information, see Checking connection between Avaya Aura Conferencing and System Manager on page 638.

## About this task

⚠ **Warning:**

> If the Meeting Exchange or imported Avaya Aura® Conferencing data contains duplication, conference names that are greater than 30 characters, or non-recognizable symbols, the migration tool applies the following changes:
>
> - Duplicate conferences, where the combination of participants and conference telephone number is the same, are removed. All clients that reference duplicate conferences are changed to reference only one conference.
> - Only alphanumeric data and the underscore (_) symbols are recognized. All other symbols are replaced with an underscore (_).
> - Conference names are truncated at 30 characters.
> - Duplicate user names are automatically corrected by appending a number to the name during the import process.
> - Duplicate conference names are automatically corrected by appending a _renamed to the name during the import process.

Use the following procedure to import the Meeting Exchange or Avaya Aura® Conferencing data that you previously exported.

## Procedure

1. **(Optional)** If the migration tool is not already open, click the **Start** menu, and select **Programs** > **Avaya** > **AAC Data Migration Tool**.
2. In the Welcome window, click **Import**.
3. In the Import dialog box, in the AAC Server section, complete the following:
    - **Host name or IP address**: Type the hostname or IP address of the Avaya Aura® Conferencing Provisioning (PROV) client. This is an administrative interface that you can use to manage your system data.
    - **Username**: Type **admin**.
    - **Password**: Type the admin password.
4. Click **Test Connection** and confirm that the message **Connected OK** is displayed.
5. In the Storage section, click the ellipsis **(...)** to specify a location to save your imported Avaya Aura® Conferencing or Meeting Exchange data.
6. Click **Import**.

7. In the **Import Parameters** dialog box, complete the following:

| Field | Action |
|---|---|
| Turnkey checkbox | Do not select. |
| Session Manager (SMName) | Enter the Session Manager name used for Avaya Aura® Conferencing as specified in System Manager. |
| Default password | You can retain the default password or enter a new one. This is the default password that the migration tool will allocate to each user for logging in to the Collaboration Agent interface. |
| Domain Name | You can enter a new domain or select a domain from the list. If your domain name is not in the list. The migration tool uses the domain name to create qualified user names for Avaya Aura® Conferencing. For example, user1@domain.com. |
| New domain checkbox | Select if you want to enter a new domain. |
| Location | You can enter a new location or select a location from the list. |
| New location checkbox | Select if you want to enter a new location. |
| Timezone | Select a timezone from the list. |

8. Click **Next**.

   An information dialog is displayed.

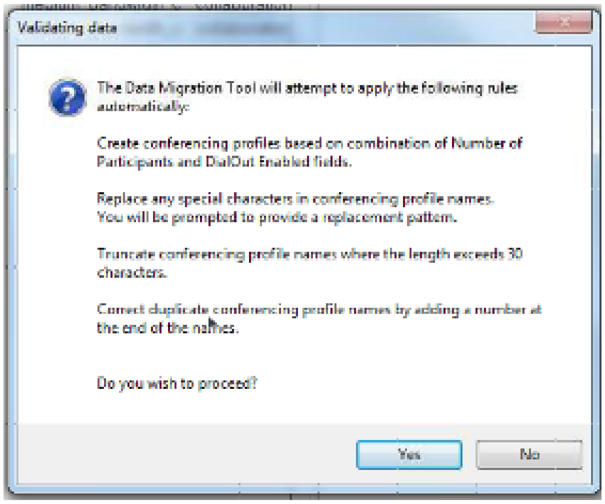
9. Click **Close** on the information dialog.

   The Create Conferencing Profiles window is displayed with the imported conference names in the left pane and the Avaya Aura® Conferencing Conferencing Profiles in the right pane.

10. Click **Validate Data** prior to importing the data into Avaya Aura® Conferencing to check for duplicate names or invalid characters in names.

    The **Validating Conference data** dialog box is displayed with the following message:

    ```
    The Data Migration Tool will attempt to apply the following rules
    automatically:
    Create conferencing profiles based on combination of Number of
    Participants and DialOut Enabled fields.
    Replace any special characters in conferencing profile names.
    You will be prompted to provide a replacement pattern.
    Truncate conferencing profile names where the length exceeds 30
    characters.
    Correct duplicate conferencing profile names by adding a number at
    the end of the names.
    Do you wish to proceed?
    ```



The Data Migration Tool will attempt to apply the following rules automatically:

Create conferencing profiles based on combination of Number of Participants and DialOut Enabled fields.

Replace any special characters in conferencing profile names. You will be prompted to provide a replacement pattern.

Truncate conferencing profile names where the length exceeds 30 characters.

Correct duplicate conferencing profile names by adding a number at the end of the names.

Do you wish to proceed?

**Figure 32: Validation dialog**

11. In the **Validating Conference data** dialog box, click **Yes** to proceed with data validation.

    If an invalid special character is found, the **Define replacement pattern** dialog box is displayed.

12. **(Optional)** In the **Enter replacement pattern here** field, type a character that replaces the invalid special character, for example, underscore (_), and click **OK**.

    ⚠ **Warning:**

    Invalid characters are automatically replaced with the pattern you provide.

13. In the **Validating Conference data** dialog box, at the message **Conference validation complete**, click **Close**.

    This dialog contains a report of all the actions that the migration tool completed.

14. On the **Validating data** dialog box, click **OK**.

    The **Create Conferencing Profiles** window appears with the remaining imported conference names in the left pane and the Avaya Aura® Conferencing Conferencing Profiles in the right pane.

15. Double-click a field to edit duplicate names or invalid characters.

    All fields can be edited, except for the **Comment** field.

    There are three new fields. These fields represent new features in this release of Avaya Aura® Conferencing which were not present in the older systems. They are:

    - **Conference Flow**
    - **Event Conference**
    - **Participant Passcode Required**

    If you edit any fields, you must validate the data again.

16. Click **Validate Data**, and click **Yes** to proceed with data validation.

The **Validating Conference data** dialog box is displayed.

17. Click **Close** when the **Conference validation complete** message is displayed.
18. Click **OK**.
19. Select the conferences in the left pane, and click **Import Selected** or **Import All**.

    The conferences on the left pane move to the right pane.
20. Click **Close**.
21. Click **Next**.
22. Click **Yes** to skip to the user templates import or click **No** to continue with conference import.

    The **Create User Templates** window is displayed in the left pane and the Avaya Aura® Conferencing User Templates are displayed in the right pane. User templates are also known as conferencing profiles. Each template is a collection of settings which you can later allocate to specific users. For example, you may wish to enable video conferencing for some users and not for other users.
23. Click **New** to create new user template(s)
24. Type the name of each template and configure the other parameters.
25. On the **Import User Templates** dialog box, click **Import Selected** or **Import All**.

    The user templates on the left pane move to the right pane.

    An information dialog is displayed.
26. Click **Close** on the information dialog.
27. Click **Next**.

    The **Load System manager user accounts** dialog box is displayed.
28. Click the ellipsis **(...)** to browse to the folder containing the System Manager user account information.

    **Note:**

    This is the path containing the stored set of XML files that were created when exporting users from System Manager.
29. On the **User Accounts** dialog box, click **OK** to perform a manual association or click **Cancel** to skip mapping to System Manager Accounts.

    If you select **Cancel**, the **Select System Manager Account** dialog box is displayed.
30. **(Optional)** Double-click on a user account to manually perform user association, and click **OK**.
31. **(Optional)** In the **Search** field, type a name or part of a name, surname, or email.

    **Note:**

    The search is case sensitive and display any matches as you type.

32. **(Optional)** Select an account, and click **OK**.

    **Note:**

    If preparing an XML file for import, if the Meeting Exchange or older Avaya Aura® Conferencing user has a System Manager account associated with it then the System Manager user account information is updated with the conferencing profile from Meeting Exchange or Avaya Aura® Conferencing and saved to the XML file.

    If there is a matching System Manager account, the following fields (in bold type) are updated:

    <commProfile xsi:type="ns9:MmcsCommProfileType" xmlns:ns9="http://xml.avaya.com/schema/import_mmcs">

    <**ns9:template**> </**ns9:template**>

    <**ns9:securityCode**> </**ns9:securityCode**>

    <**ns9:moderatorPin**> </**ns9:moderatorPin**>

    <commProfile>

    If there is no matching System Manager account, only the following fields (in bold) are updated:

    <commProfile xsi:type="ns6:SessionManagerCommProfXML"mlns:ns6="http://xml.avaya.com/schema/import_sessionmanager>

    <**ns6:primarySM**> </**ns6:primarySM**>

    <**ns6:homeLocation**> </ **ns6:homeLocation**>

    </commProfile>

    <handle>

    <**handleName**> </**handleName**>

    <**domainName**> </**domainName**>

    </handle>

33. **(Optional)** Save the user data in an XML file based on the template XML file. You can save selected records or save all records to an XML file for System Manager.

34. **(Optional)** On the **Save As** dialog box, type a name for the file such as BulkImport.xml and navigate to a location to save the file, and click **Save**.

    The Preparing Bulk Import file for System Manager window appears and indicates the number of clients that successfully saved.

35. **(Optional)** Click **Finish**.

36. Verify that there is a connection between Avaya Aura® Conferencing and System Manager prior to importing the data to System Manager. For more information, see Checking connection between Avaya Aura Conferencing and System Manager on page 638.

37. Log on to System Manager as admin to import the BulkImport.xml file into System Manager.

    **Note:**

    For more information about using the Bulk Import and Export, see *Administering Avaya Aura® System Manager*.

38. On the System Manager console, click **Services** > **Bulk Import and Export**.
39. In the navigation pane, click **Import** > **User Management** > **Users**.
40. On the Import users dialog box, in the File selection section, click **Browse**.
41. Select the BulkImport.xml file that you previously saved.

    You can monitor the status in the Manage job section.

42. Upon successful completion, return to the migration tool.
43. On the **System Manager Bulk Import Users** dialog box, click **OK**.
44. Click **Assign Selected** or **Assign All**, to assign System Profile, Participant, and Moderator codes for the users.
45. Click **Close**.
46. Click **Back to Main** to return to the main window.
47. Exit the application.

    A Web browser window automatically opens and the log file containing the details of the data manipulations is saved in HTML format.

### Result

The import is complete.

## Importing data to Avaya Aura® Conferencing for Turnkey

This process involves the following:

- Defines a domain which is appended to the qualified username for Avaya Aura® Conferencing, for example, user1@domain.com.
- Defines a user's location, user's timezone, and SIP routing tool name.
- Imports Meeting Exchange the on-demand conference data and user templates into Avaya Aura® Conferencing profiles. The migration tool does not import the scheduled conference data.

## About this task

⚠ **Warning:**

If the Meeting Exchange or imported Avaya Aura® Conferencing data contains duplication, conference names that are greater than 30 characters, or non-recognizable symbols, the migration tool applies the following changes:

- Duplicate conferences, where the combination of participants and conference telephone number is the same, are removed. All clients that reference duplicate conferences are changed to reference only one conference.
- Only alphanumeric data and the underscore (_) symbols are recognized. All other symbols are replaced with an underscore (_).
- Conference names are truncated at 30 characters.
- Duplicate user names are automatically corrected by appending a number to the name during the import process.
- Duplicate conference names are automatically corrected by appending a _renamed to the name during the import process.

Use the following procedure to import the Meeting Exchange or Avaya Aura® Conferencing data that you previously exported.

## Before you begin

- Export the data from Meeting Exchange or the older version of Avaya Aura® Conferencing.
- Install the latest release of Avaya Aura® Conferencing.
- Check to ensure that Avaya Aura® Conferencing is connected to your telecommunication central management system.

## Procedure

1. **(Optional)** If the migration tool is not already open, click the **Start** menu, and select **Programs** > **Avaya** > **AAC Data Migration Tool**.
2. In the Welcome window, click **Import**.
3. In the Import dialog box, in the AAC Server section, complete the following:
   - **Host name or IP address**: Type the hostname or IP address of the Avaya Aura® Conferencing Provisioning (PROV) client. This is an administrative interface that you can use to manage your system data.
   - **Username**: Type **admin**.
   - **Password**: Type the admin password.
4. Click **Test Connection** and confirm that the message **Connected OK** is displayed.
5. In the Storage section, click the ellipsis **(...)** to specify a location to save your imported Avaya Aura® Conferencing or Meeting Exchange data.
6. Click **Import**.
7. In the **Import Parameters** dialog box, complete the following:

| Field | Action |
|---|---|
| Turnkey checkbox | Select this checkbox. |
| Default password | You can retain the default password or enter a new one. This is the default password that the migration tool will allocate to each user for logging in to the Collaboration Agent interface. |
| Domain Name | You can enter a new domain or select a domain from the list. If your domain name is not in the list. The migration tool uses the domain name to create qualified user names for Avaya Aura® Conferencing. For example, user1@domain.com. |
| New domain checkbox | Select if you want to enter a new domain. |
| Location | You can enter a new location or select a location from the list. |
| New location checkbox | Select if you want to enter a new location. |
| Timezone | Select a timezone from the list. |

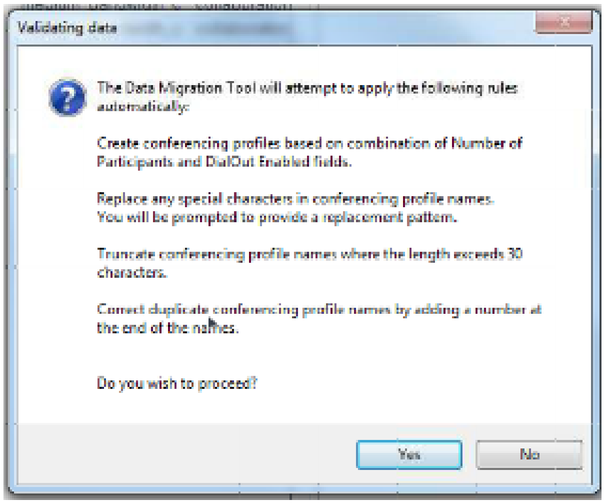
8. Click **Next**.

   An information dialog is displayed.

9. Click **Validate Data** prior to importing the data into Avaya Aura® Conferencing to check for duplicate names or invalid characters in names.

   The **Validating Conference data** dialog box is displayed with the following message:

   ```
   The Data Migration Tool will attempt to apply the following rules
   automatically:
   Create conferencing profiles based on combination of Number of
   Participants and DialOut Enabled fields.
   Replace any special characters in conferencing profile names.
   You will be prompted to provide a replacement pattern.
   Truncate conferencing profile names where the length exceeds 30
   characters.
   Correct duplicate conferencing profile names by adding a number at
   the end of the names.
   Do you wish to proceed?
   ```



Validating data

The Data Migration Tool will attempt to apply the following rules automatically:

Create conferencing profiles based on combination of Number of Participants and DialOut Enabled fields.

Replace any special characters in conferencing profile names. You will be prompted to provide a replacement pattern.

Truncate conferencing profile names where the length exceeds 30 characters.

Correct duplicate conferencing profile names by adding a number at the end of the names.

Do you wish to proceed?

**Figure 33: Validation dialog**

10. In the **Validating Conference data** dialog box, click **Yes** to proceed with data validation.

    If an invalid special character is found, the **Define replacement pattern** dialog box is displayed.

11. **(Optional)** In the **Enter replacement pattern here** field, type a character that replaces the invalid special character, for example, underscore (_), and click **OK**.

    ⚠ **Warning:**

    Invalid characters are automatically replaced with the pattern you provide.

12. In the **Validating Conference data** dialog box, at the message **Conference validation complete**, click **Close**.

    This dialog contains a report of all the actions that the migration tool completed.

13. On the **Validating data** dialog box, click **OK**.

    The **Create Conferencing Profiles** window appears with the remaining imported conference names in the left pane and the Avaya Aura® Conferencing Conferencing Profiles in the right pane.

14. Double-click a field to edit duplicate names or invalid characters.

    All fields can be edited, except for the **Comment** field.

    There are three new fields. These fields represent new features in this release of Avaya Aura® Conferencing which were not present in the older systems. They are:

    - **Conference Flow**
    - **Event Conference**
    - **Participant Passcode Required**

    If you edit any fields, you must validate the data again.

15. Click **Validate Data**, and click **Yes** to proceed with data validation.

The **Validating Conference data** dialog box is displayed.

16. Click **Close** on the information dialog.

    The Create Conferencing Profiles window is displayed with the imported conference names in the left pane and the Avaya Aura® Conferencing Conferencing Profiles in the right pane.

17. Click **OK**.
18. Select the conferences in the left pane, and click **Import Selected** or **Import All**.

    The conferences on the left pane move to the right pane.

19. Click **Close**.
20. Click **Next**.
21. Click **Yes** to skip to the user templates import or click **No** to continue with conference import.

    The **Create User Templates** window is displayed in the left pane and the Avaya Aura® Conferencing User Templates are displayed in the right pane. User templates are also known as conferencing profiles. Each template is a collection of settings which you can later allocate to specific users. For example, you may wish to enable video conferencing for some users and not for other users.

22. Click **New** to create new user template(s)
23. Type the name of each template and configure the other parameters.
24. On the **Import User Templates** dialog box, click **Import Selected** or **Import All**.

    The user templates on the left pane move to the right pane.

    An information dialog is displayed.

25. Click **Close** on the information dialog.
26. Click **Next** to import the actual users into the templates that you have created.

    The **Import Users** dialog is displayed. It contains a list of all the users on the old system. There are a number of new fields. These fields represent new features in this latest release of Avaya Aura® Conferencing which were not present in the older systems.

27. Click **Validate Data**, and click **Yes** to proceed with data validation.

    The **Validating Conference data** dialog box is displayed.

28. Click **Import Selected to AAC** or **Import All to AAC** to import the actual users.
29. Click **Close** on the information dialog.
30. Click **Finish**.

# Appendix C: Re-IPing the Application Server

## Introduction to re-IPing the Avaya Aura® Conferencing servers

This section provides the procedures to change the IP address on the Avaya Aura® Conferencing (AAC) system.

### Prerequisites

- Examine the system certificates to determine if new certificates are required.

  **Important:**

  Network elements require a new certificate if the certificate currently in use contains the old IP address or host name as the Subject AltName or the Common Name. If you want to update any other information, a new certificate is optional. However, Avaya recommends that you obtain a new certificate to keep your certificate information current.

- Obtain and install new certificates.

## Checklist for re-IPing an Avaya Aura® Conferencing system

The following checklist provides a high level view of the steps required to change the IP address of the Avaya Aura® Conferencing system.

Perform the procedure for each task in the order specified.

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 1 | Prepare your data for the re-IP | Preparing your data for the re-IP (Main method) on page 652 | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| 2 | Stop and undeploy all the network element instances except Element Manager. | Stopping a network element instance on page 659 and Undeploying a network element instance on page 659 | | |
| 3 | Stop the Element Manager instances. | Stopping an Element Manager Instance on page 660 | | |
| 4 | Remove security hardening on each server if the system uses ACL. | Configuring Access Control List to system default on page 661 | | |
| 5 | Stop the database on the primary Element Manager server.<br>**Note:**<br>For system with redundancy: Stop database on the secondary Element Manager server as well. | Stopping the database on the Element Manager server on page 661 | | |
| 6 | Update IP addresses on each server. | Updating IP addresses for the server on page 662 | | |
| 7 | Update the hostname, NTP and DNS servers on each server. | Updating the hostname and clock source on page 663 | | |
| 8 | Update Element Manager, database and network element IP addresses on the Primary Element Manager server. | Updating Element Manager database and network element IP addresses on page 665 | | |
| 9 | Update the service FQDNs. | Updating service FQDNs on page 667 | | |
| 10 | Generate new certificates for all of the network element instances. | Creating Network Element certificates signed by the System Manager on page 564 | | |
| 11 | Assign new certificates to all of the network element instances. | • Assigning a new certificate to the Element Manager on page 570<br>• Assigning a new certificate to the Collaboration Agent Manager on page 571<br>• Assigning a new certificate to the Application Server on page 567<br>• Assigning a new certificate to the Provisioning Manager on page 571<br>• Assigning a new certificate to the Web Conferencing Server on page 573 | | |

*Table continues…*

| # | Task | Description | Notes | ✔ |
|---|---|---|---|---|
| | | • Assigning a new certificate to the Web Conferencing Management Server on page 573<br>• Assigning a new certificate to the DCS on page 272<br>• Assigning a new certificate to the Avaya Media Server on page 568 | | |
| 12 | Stop the element manager instances. | Stopping an Element Manager Instance on page 660 | | |
| 13 | Update the Access Control List (ACL) configuration if the system uses ACL. | Configuring ACL on page 668 | | |
| 14 | Start the Element Manager instances. | Starting an Element Manager instance from the server console on page 669 | | |
| 15 | Deploy and start all the Network Element instances except Element Manager. | Deploying a Network Element instance on page 244 and Starting a network element instance on page 669 | | |
| 16 | Reconfigure single-sign on the System Manager to use new FQDNs/IP addresses | Configuring single sign-on for Element Manager Console and Provisioning Client on page 304 | | |

**Related links**

Preparing your data for the re-IP (Main method) on page 652
Stopping a network element instance on page 659
Undeploying a network element instance on page 659
Stopping an Element Manager instance on page 660
Configuring Access Control List to system default on page 661
Stopping the database on the Element Manager server on page 661
Updating IP addresses for the server on page 662
Updating the hostname, NTP (clock source), and DNS servers on page 663
Updating Element Manager, database, and network element IP addresses on page 665
Updating service FQDNs on page 667
Configuring ACL on page 668
Starting an Element Manager instance from the server console on page 669
Starting a network element instance on page 669

## Preparing your data for the re-IP (Main method)

Avaya recommends that you use this main method for preparing your data for the re-IP. This main method uses a job aid worksheet for gathering your data and planning your systems for the re-IP process. The job aid is called *AAC ReIP Job Aid.xlsm* and is available from https://support.avaya.com/.

The job aid worksheet has the following three tabs:

- Server Data: Enter the old and new information for each server in the system that requires a re-IP
- Application Data: Populate all the old and new IP addresses in the system.
- Role Data: Capture all the user information for server access and administration information for each server in the system requiring a re-IP.

There is also an alternative method of preparing your data for the re-IP. The alternative method is best suited to experienced administrators.

**Related links**

Checklist for re-IPing an Avaya Aura Conferencing system on page 649
Preparing server data on page 652
Preparing application data on page 653
Preparing role data on page 656
Preparing your data for the re-IP (Alternative method) on page 657

## Preparing server data

### Before you begin

Download the Job Aid, as described in Preparing your data for the re-IP (Main method) on page 652.

### About this task

Use the following procedure to populate the server data for all servers undergoing an IP address change.

### Procedure

1. Open the job aid worksheet, and click the **Server Data** tab.
2. If the hostname changes, type the Old Hostname and the New Hostname.
3. In the Internal OAM (Default) section, complete the following:
    a. Old IP address and the New IP address
    b. Old Subnet Prefix length and the New Subnet Prefix length (if the network prefix is different)
    c. Old Subnet Default Router and the New Subnet Default Router (if the default Gateway is different).

4. In the Media section, complete the following:
    a. Old IP address and the New IP address.
    b. Old Subnet Prefix length and the New Subnet Prefix length.
    c. Old Subnet Default Router and the New Subnet Default Router.

    **Note:**

    For small (SMB) and medium layouts, use the Media section of the EM Server table and for large layouts use the Media section of the MWC Server table.
5. In the EM server section for EMServer1 and EMServer2, complete the following:
    a. Old External clock Source #1 and New External Clock Source #1.
    b. Old External clock Source #2 and New External Clock Source #2 (if applicable).
    c. Old Secondary Clock Source and New Secondary Clock Source.
6. In the MWC Server section, complete the following:
    a. Old Primary Clock Source and New Primary Clock Source.
    b. Old Secondary Clock Source and New Secondary Clock Source.

    If the EMServer1 and EMServer2 IP addresses changed and the network element server undergoing a reIP uses the Element Manager server IP address as the NTP source, then you must update the NTP configuration of the network element server to use the new EMServer1 and EMServer2 IP addresses when updating your network configuration. For more information, see Updating the hostname and clock source on page 663.

### Next steps

Proceed to Preparing application data on page 653.

**Related links**

Preparing your data for the re-IP (Main method) on page 652

## Preparing application data

### About this task

Use the following procedure to populate the application data for all servers that are undergoing a re-IP.

### Procedure

1. Open the job aid worksheet.
2. Click the **Server Data** tab, and copy the Old IP address and New IP address data to the following cells on the **Application Data** tab.
    a. Old IP address
    b. New IP address

3. If Network Element (NE) service addresses change, perform the following:
    a. Log on to the Element Manager Console.
    b. In the navigation pane, click **Addresses**.
    c. Copy the addresses to the Old IP address column on the **Application Data** tab.
    d. In the New IP address column, type the new IP address for the NE service addresses.
    e. (Optional) Copy the Logical Name from the **Addresses** table to the Logical Name (optional) column on the **Application Data** tab.

    **Note:**

    If more rows are required, copy and paste new rows in the spreadsheet.
4. Click **Save IP Address List** to save the list to your PC with the filename IPAddr.txt.
5. Log on to EMServer1 as ntappadm through ssh or directly at the server console.
6. Transfer the IPAddr.txt file to the `/var/mcp/install` directory.
7. Use the linux command `chmod` to ensure that the IPAddr.txt file has full execute, write, and read access:

```
chmod 777 IPAddr.txt
```

8. If the Element Manager Internal OAM service IP address changes, on the **Application Data** tab in the Element Manager section, complete the following:
    a. Old Service IP Address (Internal OAM)
    b. New Service IP Address (Internal OAM)
9. If the Application Server Internal OAM service IP address changes, on the **Application Data** tab in the Application Server section, complete the following:
    a. Old Service IP Address (Internal OAM)
    b. New Service IP Address (Internal OAM)
10. If the Accounting Manager Internal OAM service IP address changes, on the **Application Data** tab in the Accounting Manager section, complete the following :
    a. Old Service IP Address (Internal OAM)
    b. New Service IP Address (Internal OAM)
11. If the Web Conferencing Server service IP changes, on the **Application Data** tab in the Web Conferencing Server 1 section, complete the following:
    a. Old Service IP Address
    b. New Service IP Address
12. If a second Web Conferencing Server exists in the system, on the **Application Data** tab in the Web Conferencing Server 2 section, complete the following:
    a. Old Service IP Address

   b. New Service IP Address

13. On the **Application Data** tab in the Primary DB section, complete the following for EMServer1 and EMServer2:

    a. Old IP Address

    b. New IP Address

14. If a secondary database exists in the system, on the **Application Data** tab in the Secondary DB section, complete the following:

    a. Old IP Address

    b. New IP Address

15. If the Element Manager FQDN changes, on the **Application Data** tab in the Element Manager section complete the following:

    a. Old Service FQDN

    b. New Service FQDN

16. If the Provisioning Manager 1 FQDN changes, on the **Application Data** tab in the Provisioning Manager 1 section complete the following:

    a. Old Service FQDN

    b. New Service FQDN

17. If the Collaboration Agent 1 FQDN changes, on the **Application Data** tab in the Collaboration Agent 1 section complete the following:

    a. Old Service FQDN

    b. New Service FQDN

18. If the Collaboration Agent 2 FQDN changes, on the **Application Data** tab in the Collaboration Agent 2 section complete the following:

    a. Old Service FQDN

    b. New Service FQDN

19. If the Web Collaboration Server 1 FQDN changes, on the **Application Data** tab in the Web Collaboration Server 1 section complete the following:

    a. Old Service FQDN

    b. New Service FQDN

20. If the Web Collaboration Server 2 FQDN changes, on the **Application Data** tab in the Web Collaboration Server 2 section complete the following:

    a. Old Service FQDN

    b. New Service FQDN

21. If the Document Conversion Server 1 FQDN changes, on the **Application Data** tab in the Document Conversion Server 1 section complete the following:
    a. Old Service FQDN
    b. New Service FQDN
22. If the Document Conversion Server 2 FQDN changes, on the **Application Data** tab in the Document Conversion Server 2 section complete the following:
    a. Old Service FQDN
    b. New Service FQDN

### Next steps

Proceed to Preparing role data on page 656.

#### Related links

Preparing your data for the re-IP (Main method) on page 652

## Preparing role data

### About this task

Use the following procedure to type the passwords for the following accounts for each server undergoing a re-IP.

### Procedure

1. Open the job aid worksheet.
2. Click the **Role Data** tab and type the Old Server IP and the New Server IP for each server undergoing a re-IP.
3. For each server, type the password for the accounts with the following roles:
    a. System Security Administrator (SSA) role, such as ntsysadm.
    b. Application Administrator (AA) role, such as ntappadm.
    c. Security Audior (SA) role, such as ntsecadm.
    d. Backup Administrator (BA) role, such as ntbackup.
    e. Database Administrator (DBA), such as ntdbadm.
4. In the EM and Prov Console administrator column, type the administrator password that is used to log in to the Element Manager Console or Provisioning Manager for the following accounts:
    a. admin
    b. admin1
    c. admin2
    d. admin3
    e. admin4

f. admin5

**Note:**

If more rows are required, copy and paste new rows in the spreadsheet.

For more information about the accounts and roles, see Administrative user roles and preconfigured accounts on page 29.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

**Related links**

Preparing your data for the re-IP (Main method) on page 652

## Preparing your data for the re-IP (Alternative method)

### About this task

Use this procedure to create the file with rules for changing the IP addresses on the Avaya Aura® Conferencing system.

### Procedure

1. Populate the following IP addresses table.

| Interface | Tag name | Old IP address | New IP address |
|---|---|---|---|
| IPv4 address of Avaya Aura® System Manager[14] | TAG_SMGR1_SVR_ADDR | | |
| IPv4 address of Avaya Aura® Session Manager[14] | TAG_ASM1_SVR_ADDR | | |
| Internal OAM (Default) IPv4 address of the primary Element Manager server | - | | |
| Service IPv4 address of Element Manager | TAG_EM_INT_OAM_SVC_ADDR | | |
| Service IPv4 address of Accounting Manager | TAG_AM1_INT_OAM_SVC_ADDR | | |
| Service IPv4 address of the application server | TAG_AS1_INT_OAM_SVC_ADDR | | |
| Media IPv4 address of the primary Element Manager server[15] | TAG_EM_SVR1_MEDIA_ADDR | | |

*Table continues…*

[14] Do not use if you have a turnkey deployment or if Avaya Aura® System Manager and Avaya Aura® Session Manager were not changed.

[15] For SMB simplex, SMB redundant, medium simplex or medium redundant deployment models only.

| Interface | Tag name | Old IP address | New IP address |
|---|---|---|---|
| IPv4 address of the primary Media Web Conferencing server[16] | TAG_MWC_SVR1_ADDR | | |
| Service IPv4 address of the primary Web Conferencing Server | TAG_WCS1_SVC_ADDR | | |
| Media IPv4 address of the primary Media Web Conferencing Server[16] | TAG_MWC_SVR1_MEDIA_ADDR | | |
| *Redundant systems* | | | |
| Internal OAM (Default) IPv4 address of the secondary Element Manager server | TAG_EM_SVR2_INT_OAM_ADDR | | |
| Media IPv4 address of the secondary Element Manager server[15] | TAG_EM_SVR2_MEDIA_ADDR | | |
| IPv4 address of the secondary Media Web Conferencing server[16] | TAG_MWC_SVR2_ADDR | | |
| Service IPv4 address of the secondary Web Conferencing Server | TAG_WCS2_SVC_ADDR | | |
| Media IPv4 address of the secondary Media Web Conferencing server[16] | TAG_MWC_SVR2_MEDIA_ADDR | | |

2. Create a IPAddr.txt file.
3. Add records for all the IP addresses on the Avaya Aura® Conferencing system from the table to the text file in the following format:

   ```
   <old_IP_address_1>, <new_IP_address_1>
   <old_IP_address_2>, <new_IP_address_2>
   ...
   ```

   For example:

   ```
   192.168.209.72, 192.168.159.251
   192.168.209.73, 192.168.159.252
   192.168.209.74, 192.168.159.253
   ```

4. Log on to the Primary Element Manager server as `ntappadm` through SSH or directly at the server console.
5. Transfer the IPAddr.txt file to the `/var/mcp/install` directory.

**Related links**

Preparing your data for the re-IP (Main method) on page 652

[16] For large simplex or large redundant deployment models only.

# Stopping a network element instance

## About this task

Use this procedure to stop a network element instance.

## Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > **<network element type>** > **<network element instance you want to stop** > **NE Maintenance**.
2. In the Maintenance window, select the row that has a value of the target instance in the ID column.
3. Click **Stop**.

   The **Maint** state changes from **None** to **Stopping**, indicating that the stop operation is in progress. When the stop operation is complete, the following state changes occur:

   - The **Maint** state changes back to **None**.
   - The **Admin** state changes from **Online** to **Offline**.
4. Close the Maintenance window.

## Result

The network element instance is stopped.

## Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

### Related links

Checklist for re-IPing an Avaya Aura Conferencing system on page 649

# Undeploying a network element instance

## About this task

Use this procedure to undeploy a network element instance.

## Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements**> ***<network element type>*** > ***<network element instance you want to stop>*** > **NE Maintenance**.
2. In the Maintenance window, select the row that has a value of the target instance in the ID column.

3. Click **Undeploy**.

   The Maint state changes from **None** to **Undeploying**, indicating that the undeploy operation is in progress. When the undeploy operation is complete, the Maint state changes back to **None**.

4. Close the Maintenance window.

### Result

The network element instance is undeployed.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

#### Related links

Checklist for re-IPing an Avaya Aura Conferencing system on page 649

## Stopping an Element Manager instance

### About this task

Use this procedure to stop a network element instance of Element Manager.

### Procedure

1. In the navigation pane of Element Manager Console, select **Feature Server Elements**> **Element Manager** > **Element Manager** > **NE Maintenance**.
2. In the NE Maintenance window, select the row for the primary instance of Element Manager (EM_0).
3. Click **Stop**.

   The Confirmation dialog box appears, prompting you to confirm that you want to stop the active Element Manager.

4. In the Confirmation dialog box, click **OK**.
5. Close the Maintenance window.

### Result

The network element instance is stopped.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

#### Related links

Checklist for re-IPing an Avaya Aura Conferencing system on page 649

## Configuring Access Control List to system default

### About this task

Use the following procedure for each server in the system with Access Control List (ACL) previously configured.

### Procedure

1. Log on to the server as ntsysadm through ssh or directly on the server console.
2. Type `iptcfg`, and press **Enter**.
3. At the prompt, `password for ntsysadm`, type the password, and press **Enter**.
4. On the IPTables configuration Options screen, perform the following:
    a. Type `7` to select **Restore System Default**, and press **Enter**.
    b. Type `y` to proceed, and press **Enter**.
    c. Type `9` to exit, and press **Enter**.
    d. Type `y` to proceed to exit, and press **Enter**.

### Next steps

Proceed to updating IP addresses for the server.

**Related links**

Checklist for re-IPing an Avaya Aura Conferencing system on page 649

## Stopping the database on the Element Manager server

### About this task

Use the following task to stop the database on the Element Manager server.

### Procedure

1. Log on to the database server as `ntsysadm` or an account with the SSA role through SSH or directly on the server console.
2. Type `stopDB` to stop the hosted database server instance, and press **Enter**.
3. Type `statusOfDB` to verify that the database has stopped, and press **Enter**.

### Result

The database on the Element Manager server stops.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

**Related links**

Checklist for re-IPing an Avaya Aura Conferencing system on page 649

## Updating IP addresses for the server

### About this task

Use the following procedure to change the IP address of the servers in your system. Perform this procedure for every server undergoing an IP address change.

**Note:**

If the Avaya Aura® Conferencing system is moving to a different network, ensure the Avaya Aura® Conferencing system is connected to the new network before proceeding.

### Procedure

1. Log on to the database server as ntsysadm or an account with the SSA role through SSH or directly on the server console.
2. Type `mcpShowNwkConfig` to determine the network configuration, and press **Enter**.
3. Add the new internal OAM IP address:

   ```
   mcpModIPv4Subnet —name <subnet name> -addr <new internal OAM IP
   address>/<new internal SOM IP subnet prefix> -router <subnet
   default router>
   ```

   For example:

   ```
   mcpModIPv4Subnet -name sn0 -addr 192.168.159.251/16 -router
   192.168.159.1
   ```

   **Note:**

   Your connection with this server may be interrupted if this subnet is modified. If the interruption occurs, you will need to re-login the server.
4. If you have a SMB or medium size deployment, with or without redundancy:
   a. Remove the old media address

   ```
   mcpModIPv4Subnet -name <subnet name>-delotheraddrs <old media
   address>
   ```

   For example:

   ```
   mcpModIPv4Subnet -name sn0 -delotheraddrs 192.168.209.73
   ```

   b. Add a new media address

   ```
   mcpModIPv4Subnet -name <subnet name>-addotheraddrs <new media
   address>
   ```

   For example:

```
mcpModIPv4Subnet -name sn0 -addotheraddrs 192.168.159.253
```

5. Type `mcpShowNwkconfig` to verify modification of the network configuration, and press **Enter**.

### Result

The IP addresses are configured on the server.

**Related links**

Checklist for re-IPing an Avaya Aura Conferencing system on page 649

## Updating the hostname, NTP (clock source), and DNS servers

### About this task

Use the following task to update the hostname, NTP, and DNS servers in your system. Perform this procedure for every server undergoing an IP address change.

### Procedure

1. Log on to the database server as ntsysadm or an account with the SSA role through SSH or directly on the server console.
2. Type `su -` to log on as root, and press **Enter**.
3. Type `reconfigure.pl`, and press **Enter**.
4. Type the SAA password, if prompted, and press **Enter**.
5. Type <*new FQDN*>.
6. At the prompt to confirm, type `y`, and press **Enter**.
7. At the prompt `Do you want to configure DNS Client? (Y/N) [Y]`, type **y** and press **Enter**.

   . The following prompt is displayed:

   ```
   Please select one of the following actions:
   - [A]dd Domain Suffix(es)
   - Re[S]elect all Domain Suffix(es)
   - [C]ontinue
   ```
8. At the prompt, type `c` to continue or `a` to add suffixes, and press **Enter**.
9. At the prompt `How many DNS Servers would you like to reference (1-3) [1]`, type the number of available DNS servers, and press **Enter**.
10. At the prompt `Enter DNS Server`, type the IP address of the DNS server, and press **Enter**.
11. At the prompt `You entered "<IP address>" Is this correct? (Y/N) [N]`, verify the IP address.
12. If the IP address is correct, type `y` and press **Enter**.

13. At the prompt to use the default value for this timezone, type `y`, and press **Enter**.
14. At the prompt, `Do you wish to configure/display the Audit configuration?`, type `q`, and press **Enter**.
15. At the prompt, `Do you wish to configure/display Inactive Login Audit configuration?`, type `q`, and press **Enter**.
16. At the prompt, `Do you wish to configure/display the NTP configuration?`, type `c`, and press **Enter**.
17. Specify the clock source function of the server, select one of the following, and press **Enter**:

    ```
    a. Primary Clock Source server (primary Element Manager server machine). For
    example, EMServer1.
    b. Secondary Clock Source server (secondary Element Manager server machine). For
    example, EMServer2.
    c. This server is NOT a Clock Source server (all other server machines). If you
    select this option, continue to Step 5 on page 124.
    Select an option (1-3):
    ```

    Select from those options and press Enter:

    - Choose Option 1 if the server is EMServer1 (primary Element Manager server)
    - Choose Option 2 if the server is EMServer2 (secondary Element Manager server)
    - Choose Option 3 if the server is MWC server (for a Large configuration) (If you select this option, skip to step 26)
18. If you selected EMServer1 or EMServer2, configure the external clock source. The primary clock source server requires an external clock.

    At the following prompt, type `e` and press **Enter**.

    ```
    Select External Clock for time source(s) external to this server.
    Select Internal clock to use the system clock as the time source.
    E — External Clock Source (IP Addresses)
    I — Internal Clock (Unreliable)
    ```
19. At the prompt, `How many external clock sources would you like to reference (1-2) [1]?`, perform one of the following:

    - If you have defined both the external clock sources (new External Clock Source #1 and new External Clock Source #2) in the Job Aid Worksheet, type `1` and press **Enter**.
    - If you have defined only one External Clock Source in the Job Aid Worksheet, type `2` and press **Enter**.

    **Note:**

    There must be at least one external clock source defined for an Element Manager server.
20. At the prompt, `External Clock Source IP address #1` type the IP address for the external clock source. If you have more than one clock source, a second prompt is displayed.

21. At the prompt, `Would you like to configure symmetric key authentication for server New External Clock Source #1?`, type `n`.
22. Repeat the last two steps for New External Clock Source #2, if you are using it.
23. For Element Manager Server 1, at the prompt, `Enter the Machine Logical IP address of the Secondary Clock Source Server`, type the New Secondary Clock Source address and press **Enter**.

    **Note:**

    If this is a simplex (non-redundant) system, enter this server's MACHINE Logical IP address as the New Secondary Clock Source address.
24. For Element Manager Server 2, at the prompt, `Enter the Machine Logical IP address of the Primary Clock Source Server`, type the New Primary Clock Source address and press **Enter**.
25. At the prompt, `Is this information correct? Y/N [N]`, type `y` to continue or `n` to correct.
26. For the MWC server (and other element servers, if any), perform the following:
    a. At the prompt, `Enter the Machine Logical IP address of the Primary Clock Source Server`, type the New Primary Clock Source address, and press **Enter**.
    b. At the prompt, `Enter the Machine Logical IP address of the Secondary Clock Source Server`, type the New Secondary Clock Source address, and press **Enter**.
    c. At the prompt to verify the NTP configuration, type Y, and press **Enter**.
27. At the prompt, `Grub password configuration`, type `q` and press **Enter**.
28. At the prompt, `SysLog Configuration`, type `q`, and press **Enter**.

### Next steps

Proceed to update the Element Manager, database and network element IP addresses.

**Related links**

Checklist for re-IPing an Avaya Aura Conferencing system on page 649

## Updating Element Manager, database, and network element IP addresses

### About this task

Use this procedure to update the IP addresses for Element Manager, database, and network elements.

## Procedure

1. Log on to the database server as ntsysadm or an account with the SSA role through SSH or directly on the server console.
2. Type `su -` to log on as root, and press **Enter**.
3. Type `/etc/init.d/./reconfigDbServer`, and press **Enter**.
4. Type `su ntdbadm`, and press **Enter**.
5. Type `restartDB`, and press **Enter**.
6. Type `exit`.
7. Perform steps 1 to 6 on the secondary database.
8. Log on to EMServer1 (hosting EM instance 0) as ntappadm or an account with the AA role through SSH or directly on the server console.

   **Note:**

   If the IP address for EMServer1 changed, use the new IP address; otherwise, use the old IP address.
9. Type `cd /var/mcp/install`, and press **Enter**.
10. Type `vi installprops.txt` to edit, and type the New IP address for the following (if changed):
    a. For EMServer1, in the **ne.mgmt.ip** field, type the New IP address in the Internal OAM network of the EM Server 1.
    b. For the server hosting the Primary database, in the **db.host** field, type the New IP address in the Internal OAM network of the Primary Database.
    c. For the server hosting the Secondary database, in the **db.secHost** field, type the New IP address in the Internal OAM network of the Secondary Database.
11. Type `./dbInstall.pl –fo`, and press **Enter**. The script displays the database settings.
    a. At the prompt, `Continue with these settings? (Y/N) [N]`, type `y`, and press **Enter**.
    b. At the prompt, `Perform "Deploy Files Only" operation to Secondary DB (Y/N) [N]`, type `y`, and press **Enter**.
12. Type `./emDeploy.pl`, and press **Enter**.

    The script displays the Element Manager settings.
13. At the prompt, `Continue with these settings? (Y/N) [N]`, type `y`, and press **Enter**.
14. Type `./addrListUpdate.pl –i IPAddr.txt`, and press **Enter**.
15. Type `./emStart.pl`, and press **Enter**.

### Result

Element Manager, the database, and all the network elements now have new IP addresses.

#### Related links

Checklist for re-IPing an Avaya Aura Conferencing system on page 649

## Updating service FQDNs

You can edit the Fully Qualified Domain Name (FQDN) of the various network elements using the Element Manager Console. You can edit the FQDN of the Element Manager, the Provisioning Manager, the Document Conversion Server (DCS), the Web Conferencing Server (WCS), the LDAP server, and/or Collaboration Agent Managers. The process of editing the FQDNs of the various network elements is essentially the same for each network element.

### Before you begin

Ensure that you download and populate the Job Aid worksheet. The job aid is called *AAC ReIP Job Aid.xlsm* and is available from https://support.avaya.com/.

### About this task

Use this task to update the service FQDN for Element Manager and other network elements.

### Procedure

1. Log on to the Element Manager Console.
2. Navigate to **Feature Server Elements** > **Element Manager**
3. In the Element Manager window, select the Element Manager and click **Edit**.
4. In the **Edit Element Manager** dialog, update the Element Manager Service FQDN with the FQDN from the Job Aid Worksheet.
5. Click **Apply**.
6. In the navigation pane of Element Manager Console, click **Feature Server Elements > Provisioning Managers**.
7. In the Provisioning Managers window, select **PROV1**.
8. Click **Edit (-/+)**.
9. In the **Edit PROV1** dialog, update the Provisioning Manager Service FQDN with the FQDN from the Job Aid Worksheet.
10. In the **Edit PROV1** dialog, update the Collaboration Agent Service FQDN with the FQDN from the Job Aid Worksheet.
11. Click **Apply**.
12. In the Provisioning Managers window, select **PROV2**.
13. Click **Edit (-/+)**.

14. In the **Edit PROV2** dialog, update the Provisioning Manager Service FQDN with the FQDN from the Job Aid Worksheet.
15. In the **Edit PROV2** dialog, update the Collaboration Agent Service FQDN with the FQDN from the Job Aid Worksheet.
16. Click **Apply**.
17. Navigate to **Feature Server Elements** > **Document Conversion Servers** > **Document Conversion Servers**.
18. In the Document Conversion Servers window select the first Document Conversion Server (DCS1) and **Edit**.
19. In the **Edit DCS1** dialog, update the Document Conversion Server Service FQDN with the FQDN from the Job Aid Worksheet.
20. Click **Apply**.
21. In the Document Conversion Servers window select the second Document Conversion Server (DCS2) and **Edit**.
22. In the **Edit DCS2** dialog, update the Document Conversion Server Service FQDN with the FQDN from the Job Aid Worksheet.
23. Click **Apply**.
24. Navigate to **Feature Server Elements** > **Web Conferencing** > **Web Conferencing Servers and Clusters** > **Web Conferencing Servers**
25. In the Web Conferencing Servers window select the first Web Conferencing Servers (WCS1) and click **Edit** .
26. In the **Edit WCS1** dialog, update the FQDN with the FQDN from the Job Aid Worksheet.
27. Click **Apply**.
28. In the Web Conferencing Servers frame select the second Web Conferencing Servers (WCS2) and click **Edit** .
29. In the **Edit WCS2** dialog, update the FQDN with the FQDN from the Job Aid Worksheet.
30. Click **Apply**.

### Result

Now the FQDNs are updated for all network elements.

### Related links

Checklist for re-IPing an Avaya Aura Conferencing system on page 649

## Configuring ACL

After a server IP address change, update the Access Control List (ACL) configuration if the system uses ACL.

### Before you begin

You have a copy of the *Avaya Aura® Conferencing Security* document, which is available from Avaya Support.

### Procedure

To update the ACL configuration after an IP address change, see the instructions in the *Avaya Aura® Conferencing Security* document.

### Next steps

Proceed to starting the application.

**Related links**

Checklist for re-IPing an Avaya Aura Conferencing system on page 649

## Starting an Element Manager instance from the server console

### About this task

Use the following procedure to start the primary Element Manager, database, and other network elements.

### Procedure

1. Log on to the server hosting EM instance 0 either through ssh or the server console. At the logon prompt, type `ntappadm` or logon to an account with the AA role assigned.
2. Type `cd /var/mcp/install`, and press **Enter**.
3. Type `./emStart.pl`, and press **Enter**.

**Related links**

Checklist for re-IPing an Avaya Aura Conferencing system on page 649

## Starting a network element instance

### About this task

Use this procedure to start a network element instance.

### Procedure

1. Log on to the Element Manager Console.
2. 1. In the navigation pane of Element Manager Console, select **Feature Server Elements** > ***<network element type>*** > ***<network element instance you want to start>*** > **NE Maintenance**.
3. In the Maintenance window, select the row that has a value of the target instance in the ID column.

4. Click **Start**.

   The **Maint** state changes from **None** to **Starting**, indicating that the restart operation is in progress. When the restart operation is complete, the following state changes occur:

   - The **Maint** state changes back to **None**.
   - The **Admin** state changes from **Offline** to **Online**.
   - The **Link** state changes from **Down** to **Up**.
   - The **Oper** state changes from **Unavailable** to either **Active** or **Hot Standby**, based on the instance of the component.

5. Close the Maintenance window.

### Result

The network element instance is up and running.

### Next steps

Refer back to your checklist for more information about your next task. You should always use your checklist for guidance. You should print it out so that you can mark each task as you complete it.

**Related links**

Checklist for re-IPing an Avaya Aura Conferencing system on page 649

# Appendix D: DNS and Avaya Aura® Conferencing

## DNS and Avaya Aura® Conferencing

Typically, customers who purchase and implement the Avaya Aura® Conferencing solution also support Domain Name Server (DNS) lookup in their deployment. So, in most cases, DNS is used at a solution level for Avaya Aura® Conferencing. However, there are a small number of customers who purchase and implement Avaya Aura® Conferencing in a deployment that does not support DNS lookup. It is more likely that small to medium sized enterprises may not use DNS at a solution level for Avaya Aura® Conferencing. These customers, who do not implement DNS lookup, must manually ensure that the mapping between Fully Qualified Domain Names (FQDN) and IP addresses is accurate and up-to-date.

In the Avaya Aura® Conferencing solution, a table called **/etc/hosts** manages the mapping between domain names and IP addresses.

## Updating the host table entries

**Note:**

Perform this procedure only if the DNS client is not configured on the server.

The FQDN assigned to each Web Conferencing Service IP must be mapped to a corresponding IP address. Any server hosting a managed element instance that communicates with a Web Conferencing Service IP requires mapping.

Entries in the `/etc/hosts` table are managed by using the **`hostTableConfig`** alias. You must be logged on to an account with the SSA role (for example, ntsysadm).

### Before you begin

- You must know the mapping of the service FQDN to IP address for each Web Conferencing Service IP.
- If the Web Conferencing Service IP is located within the DMZ, ping the IP address of each server to confirm communications between all components.

**Note:**

If your firewall blocks ICMP, you cannot verify communications between all components using ping.

## About this task

Use the following procedure to create the mapping of FQDN to IP address on the Avaya Aura® Conferencing servers.

## Procedure

1. Log on to the server hosting a Web Conferencing Server using an account with the SSA role (for example, ntsysadm).
2. Type `hostTableConfig -a <IP_Address> <FQDN>` for every IP address that requires mapping.

   Where IP_Address is the IP address to map to the specific Web Conference service FQDN.
3. Repeat Step 2 for each server hosting the following Network Elements:
   - Application Server
   - Provisioning Manager
   - Collaboration Agent Manager
   - Web Conferencing Management Server
   - Web Conferencing Server
   - Recording Server(s)

   **Note:**

   Systems external to Avaya Aura® Conferencing must be able to translate the Web Conferencing Server FQDN into an IP address for routing. Contact your network engineers to configure entries on your DNS servers.

# Appendix E: Avaya Communicator for Microsoft Lync overview

Avaya Communicator for Microsoft Lync is intended for a network environment where the Microsoft Lync Server is deployed. Avaya Communicator for Microsoft Lync is a client side add-in to the Microsoft Lync 2010 and 2013, and Skype for Business 2015 and 2016. Avaya Communicator for Microsoft Lync can be used to control an H.323 or SIP desk phone or a VDI Communicator client.

Avaya Communicator for Microsoft Lync joins Avaya Aura® communications with the Lync or Skype for Business client using Microsoft supported APIs. The result is industry leading Avaya communications integrated into the look and feel of Microsoft Lync. Avaya Communicator for Microsoft Lync can interwork with a desk phone or a VDI Communicator client. Using Computer Telephony Integration (CTI), you can integrate the telephone with the computer for managing telephone calls. Using a Virtual Desktop Infrastructure (VDI) soft client, you can enhance the audio quality of voice calls by processing the audio locally on your VDI endpoint. The VDI endpoint can be a thin client or a Windows personal computer.

Avaya Communicator for Microsoft Lync provides the following operational modes:

- Desk Phone or Shared Control mode.
- Computer mode.

  **Note:**

  Computer mode is not supported when Avaya Communicator for Microsoft Lync is deployed with a VDI client.
- Other Phone mode.

For a detailed description of Avaya Communicator for Microsoft Lync functionality, see Telephony and video services with Avaya Communicator for Microsoft Lync on page 676.

Avaya Communicator for Microsoft Lync interacts with Lync 2010, Lync 2013, or Skype for Business 2015 and 2016 directly using Microsoft supported APIs. All telephony capabilities are integrated directly between Avaya Communicator for Microsoft Lync and the Microsoft Lync or Skype for Business client. You only require a Standard CAL (license), eliminating the need for a Microsoft voice infrastructure and the Microsoft Lync Enterprise CAL. Remote Call Control and Enterprise Voice must be disabled on the Lync server.

**Related links**

Avaya Communicator for Microsoft Lync features on page 674
Telephony and video services with Avaya Communicator for Microsoft Lync on page 676
Interoperability on page 680

# Avaya Communicator for Microsoft Lync features

The Avaya Communicator for Microsoft Lync solution uses the Lync 2010 and 2013 user interface to provide voice services.

**Note:**

For a detailed description of each voice service and a list of the services supported by each service provider, see Telephony and video services with Avaya Communicator for Microsoft Lync on page 676.

The solution supports the following functionality:

- Support for Computer (soft client), Desk Phone (CTI control of Desk phone), and Other Phone modes when Avaya Communicator for Microsoft Lync is interworking with a desk phone. When Avaya Communicator for Microsoft Lync is working with a VDI Communicator client, only the Desk Phone (Shared Control) and Other Phone modes are supported.
    - Using Computer Telephony Integration (CTI), you can integrate the telephone with the computer for managing telephone calls.
    - Using Virtual Desktop Infrastructure (VDI) soft client, you can enhance the audio quality of voice calls by processing the audio locally on your VDI endpoint (a thin client or a Windows personal computer).
- Make calls from Dialpad, Contact list, or search dialog box utilizing contacts published numbers.
- With Avaya Collaboration Services, make calls or send IMs from Microsoft Office applications or a web browser. For more information, see *Administering Avaya Collaboration Services* (NN10850-031).
- Translation of E.164 numbers to customer dial plan including insertion or deletion of appropriate digits.
- Publish Telephony Presences on behalf of the user when their client is signed in and on a call.
- Display a Conversation window with the following mid-call functionality:
    - Release/End call.
    - Place call on Hold and Retrieve call.
    - Insert DTMF digit in to an established call.
    - Speaker volume control and speaker mute function (Computer mode).
    - Microphone mute function (Computer mode).
    - Escalate to a video call.
- Handling multiple calls:
    - Support for multiple Consult calls.
    - While on a Consult call, instigate a Call Transfer.

  - While on a Consult call, merge another call to form a Conference call.
  - Add additional Consult calls to this Conference call.
  - Call Waiting pop-up display.
- Display an incoming call window with the following functionality:
  - Indicate the Incoming Caller line ID or Caller name.
  - Allow the user to answer or ignore the call.
  - While on a call, indicate that another call is waiting. Answering this call places the first call on Hold.
- Using EC500, you can answer Avaya Communicator for Microsoft Lync calls on your mobile device. You can also extend calls to your mobile device.
- Access the Share My Bridge feature:
  - Dial in to your conference bridge or launch web collaboration from the Avaya Communicator for Microsoft Lync bar or from a Conversation window.
  - Share conference bridge and web conference details with another user via instant message or email.
- With Bridged Line Appearance, the incoming call notification in Avaya Communicator for Microsoft Lync also indicates whether the call is intended for you or for your boss.
- Set Call Forward options.
  - Send All Calls
- Check for and access new voice mail messages.
- Make a video call when Avaya Communicator for Microsoft Lync is working with a desk phone:

  ❗ **Important:**

  The desk phone should only be H.323.

  - Escalate an existing call to a video call.
  - Start a video call.
  - Mid call control ability to block and unblock camera, and undock the Video window from the Conversation bar.
  - Incoming video call prompting to accept, or ignore incoming video and reply with an instant message.

  ✱ **Note:**

  Avaya Communicator for Microsoft Lync interworking with a VDI Communicator client does not currently support video call functionality.
- Access to call history records for incoming, outgoing, and missed calls.
- With Multiple Device Access (MDA), log in to your extension, answer calls, and join calls from multiple devices.

- With dual registration, log in to an H.323 endpoint and a SIP endpoint at the same time. You can also join calls from both devices with dual registration and extend call to a mobile device.

**Related links**

Avaya Communicator for Microsoft Lync overview on page 673

# Telephony and video services with Avaya Communicator for Microsoft Lync

Avaya Communicator for Microsoft Lync controls a single line, based on your primary line. If your desk phone supports multiple lines, non-primary lines will not be represented by Avaya Communicator for Microsoft Lync.

**Note:**

The following features are not supported:

- Single Step Transfer or Blind Transfer.
- Video when Avaya Communicator for Microsoft Lync interworks with a VDI Communicator client.

The following table lists supported functionality:

**Table 44: Telephony feature descriptions**

| Capability | Description |
|---|---|
| Make Call | You can make a call on your phone by:<br>• Clicking a contact in the contact list, and then clicking the ☎ icon in Lync 2010.<br>• Hovering over the picture of a contact and clicking the ☎ icon in Lync 2013 or Skype for Business 2015 and 2016.<br>• Using Dialpad in Avaya Communicator for Microsoft Lync 2013 and the persona menu.<br>• Entering a number in the Lync 2010, Lync 2013, or Skype for Business 2015 and 2016 dialog box.<br>**Note:**<br>With Avaya Collaboration Services, you can also make calls or send IMs from Microsoft Office applications or web browsers. For more information, see *Administering Avaya Collaboration Services (NN10850-031)*. |
| Release Call | You can release a phone call by clicking **End Call** in the Avaya Communicator for Microsoft Lync Conversation bar. |

*Table continues…*

| Capability | Description |
|---|---|
| Answer Call | You can accept an incoming call that is presented to you through an Incoming Call Notification window. |
| Ignore Call | You can ignore a phone call by clicking **Ignore Call** in the Incoming Call Notification window. |
| Escalate to a video call | You can escalate an existing audio call to a video call in the Conversation bar. The call can be in undocked or full screen mode.<br>**Note:**<br>• When an Avaya Communicator for Microsoft Lync H.323 endpoint is a party on a call, only the originator of the call can escalate an audio call to a video call. This behavior occurs regardless of whether the originator of the call is using an H.323 or SIP endpoint.<br>• In an ad-hoc conference where the moderator has a SIP endpoint and the participants have H.323 endpoints, the participants might see a Video window. |
| Reply to a video call with an IM | You can accept or ignore an incoming video call, and reply with an IM. |
| Block and unblock camera | Using the Mid-call control functionality, you can:<br>• Block or unblock camera from the Video window menu.<br>• Undock the Video window from the Conversation bar. |
| Stop video | You can stop video from the Video window menu. Stopping video does not end the call. |
| Telephony Presence | Avaya Communicator for Microsoft Lync automatically publishes telephony presence on behalf of you when you are on a call. You can still choose to manually update their presence status. |
| Caller ID | You receive Calling Party Name or Caller line ID in the Incoming Call Notification window. |
| Call forward to another phone line or voice mail | You can activate Call Forward on your PBX line for incoming calls by clicking **Call Forward** in the Avaya Communicator for Microsoft Lync bar. When the call forwarding feature is activated, you do not receive incoming call notifications. The callee that the call is forwarded to receives an incoming call notification, and after answering the call, a video request also appears.<br>**Note:**<br>When Avaya Communicator for Microsoft Lync is in Other Phone mode, call forwarding functionality is disabled. |
| EC500 | Using EC500, you can answer Avaya Communicator for Microsoft Lync calls on your mobile device. You can also extend calls to your EC500 mobile device if the Extend Calls capability is enabled in your Avaya Aura® network. |
| Send All Calls | Using Send All Calls, you can route calls to your EC500 device within your coverage area. |

*Table continues…*

| Capability | Description |
|---|---|
| Call Hold and Retrieve | Using the **Hold** button, you can put a call on hold. Click the button again to retrieve the call. |
| Generate Digits (DTMF) | You can send DTMF digits through the PBX system by selecting the **Dialpad** button on the Conversation bar.<br>This feature is disabled when:<br>• The call is on hold.<br>• Avaya Communicator for Microsoft Lync is in SIP Other Phone mode.<br>In Lync 2013 or Skype for Business 2015 and 2016, the dial pad is dimmed when disabled. In Lync 2010, the dial pad is invisible when disabled. |
| Consult Call | When on an active call, you can:<br>• Answer a call.<br>• Start a second call by:<br>- Clicking a contact in your contact list.<br>- Entering a number in the Lync 2010, Lync 2013, or Skype for Business 2015 and 2016 search box.<br>- Using the Avaya Communicator for Microsoft Lync Dialpad.<br>When another call is answered or started, the previously active call is put on hold.<br>You can create multiple consult calls. |
| Consult Transfer | When one or more consult calls are established, you can select the call you want to transfer from the list of calls on hold. |
| Consult Conference | When one or more consult calls are established, you can select the call you want to merge into a Conference call from the list of calls on hold. |
| Call Waiting | When on an active call, an Incoming Call Notification window displays, indicating that another call is waiting. If you answer this call, then current active call is put on hold. The new call becomes the active call. |
| Receiver Mute | You can mute or un-mute your PC speakers or headset receivers in Computer mode. |
| Receiver Volume Control | You can adjust the volume of the PC speakers or headset receivers in Computer mode. |
| Audio Devices Mute | You can mute or un-mute your PC speakers or headset microphones in Computer mode. |
| Make Video Call | You can make a video call by:<br>• Selecting a contact in your contact list and then clicking **Make Video Call**.<br>• Using the dial pad Lync persona menu in Lync 2013 or Skype for Business 2015 and 2016. |

*Table continues…*

| Capability | Description |
|---|---|
| | ✱ **Note:**<br>When making a video call or escalating an audio call to a video call, the IM pane does not appear in Avaya Communicator for Microsoft Lync 2013. This issue does not apply to Avaya Communicator for Microsoft Lync 2010. |
| Share My Bridge | With Avaya Communicator for Microsoft Lync 2013, you can send dial-in details and conference details to another user through IM.<br>This feature is not available in Avaya Communicator for Microsoft Lync 2010. |
| Launch My Collaboration | With Avaya Communicator for Microsoft Lync 2013, you can start a web collaboration session.<br>This feature is not available in Avaya Communicator for Microsoft Lync 2010. |
| Bridged Line Appearance | **Incoming Call Appearance:**<br>Bridged Line Appearance enhances the experience of incoming calls with bridged lines. The incoming call notification displays the name or phone number of the bridged line owner.<br>**Make Call As:**<br>You can also use Make Call As to make a call from another line.<br>✱ **Note:**<br>Exclusion is not supported. |
| Message Waiting Indication | With Avaya Communicator for Microsoft Lync, the **Message Waiting Indicator** button on the Avaya Communicator for Microsoft Lync bar lights up to indicate when you have a new voice mail message. You can click this button any time to dial in to voice mail. |
| Call History | Call history records for calls made or answered through Avaya Communicator for Microsoft Lync are saved. Avaya Communicator for Microsoft Lync also generates call history records for missed calls. |
| Multiple Device Access (MDA) | MDA provides the following capabilities:<br>• Ability to log on to the same extension from multiple SIP devices<br>• Ability to answer a call from multiple devices<br>• Ability to join an existing call from other logged in devices<br>All logged in devices ring simultaneously when an incoming call is made to the extension.<br>The Avaya Aura® network configuration, which your administrator configures, determines: |
| Dual Registration | Using Dual Registration, you can register Avaya Communicator for Microsoft Lync as an H.323 endpoint and simultaneously register a single SIP endpoint. |

**Related links**

Avaya Communicator for Microsoft Lync overview on page 673

# Interoperability

Avaya Communicator for Microsoft Lync requires certain key components to work. Avaya Communicator for Microsoft Lync can also optionally interoperate with Avaya applications including:

- Avaya Collaboration Services
- Avaya Aura® Conferencing and Collaboration Agent

⊕ **Tip:**

For easy access to Collaboration Agent web conferencing, you can select the **Remember Me** check box on the login page to save your username and password. With this option selected, you can automatically log in to your web conference without entering your credentials every time.

For additional information about Avaya Collaboration Services, see *Administering Avaya Collaboration Services* (NN10850–031).

For information about Avaya Aura® Conferencing and Collaboration Agent, see:

- *Deploying Avaya Aura® Conferencing*
- *Administering Avaya Aura® Conferencing*
- *Using Avaya Aura® Conferencing Collaboration Agent*

# Appendix F: Avaya Aura® Communicator Integration overview

## Overview

Avaya Equinox for Windows enables you to log into your company's server, and make and receive voice or video calls from your telephone extension using your computer. Using the Avaya Equinox for Windows client, you can also send instant messages, access your call history, access your Avaya Aura® contacts and Microsoft Outlook contacts, share information with web collaboration, perform an enterprise search, and manage your presence status. Avaya Equinox for Windows provides enterprise users with simple access to all the communication tools in a single interface.

Avaya Equinox for Windows provides automatic integration with Avaya Aura® Conferencing. When you log in to a MeetMe conference on Avaya Aura® Conferencing or Avaya Scopia® with Avaya Equinox for Windows, you can:

- Access the Web Collaboration features by clicking the **Collaboration** button in the main window. If you are the moderator or have presenter privileges, you can host the web collaboration session and share documents, presentations, pictures, a whiteboard, your entire screen, a portion of your screen, or an application window.
- View a graphical representation of the conference and its participants.
- Manage the conference using the built-in moderator controls when you are logged in as the moderator.

If you have Avaya Aura® Conferencing, you can also start Adhoc conferences with Avaya Equinox for Windows.

You must have access to your company's network to use Avaya Equinox for Windows.

**Related links**

Main window on page 681
Button descriptions on page 686
Multiple Device Access overview on page 687

## Main window

The following figure shows the components of the main window of Avaya Equinox for Windows. This is the compact view with no tabs expanded.

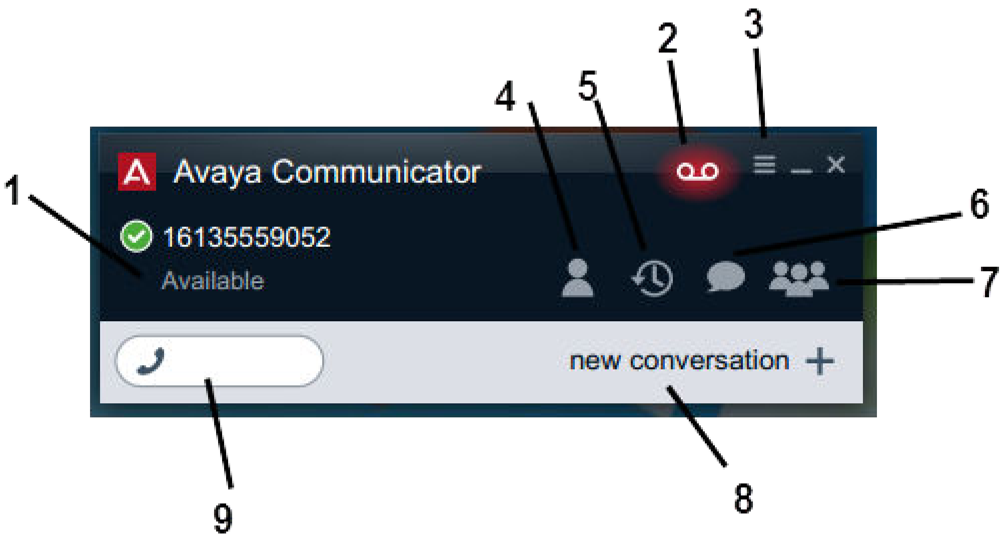


**Figure 34: Compact window**

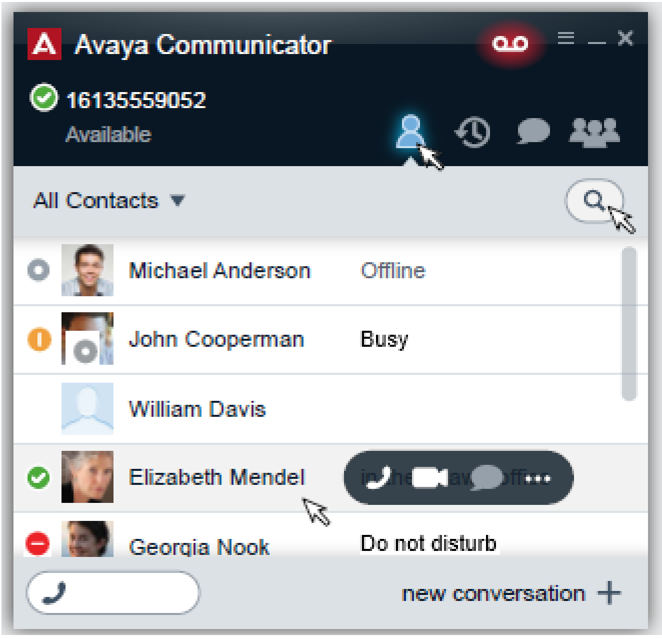
| No. | Name | Description |
|---|---|---|
| 1 | User Status area | Use this area to log in and log out of the client, and to view your extension number and presence status. From this area, you can:<br>• log in and out of the client<br>• set your presence status or enter a custom presence status message |
| 2 | **Message Waiting Indicator** | Lights up to indicate when you have a new voice mail message. You can click this button at any time to dial in to your voice mail. |
| 3 | **Options and Settings** button | You can adjust the volume from **Volume**.<br>Click **Other Settings** to configure your servers, dialing rules, enterprise directory search settings, contacts search settings, audio settings, video settings, conference settings, preferences, and messaging settings. **Other Settings** also displays the software release and support information. |
| 4 | **Contacts** tab | Displays the Contacts fan. The Contacts fan displays cards for all of your Avaya Aura® contacts and Microsoft Outlook contacts (if Microsoft Outlook is running). When the Contacts fan is expanded, you can hover over a contact to see buttons for voice call, video call, IM, and additional options.<br>If you have configured the enterprise search settings, you can also search for Communicator contacts from the Contacts tab.<br>**Note:**<br>You must be logged into the server to view your Avaya Aura® contacts and Microsoft Outlook contacts. Microsoft Outlook |

*Table continues…*

| No. | Name | Description |
|---|---|---|
| | | must be running for you to view your Microsoft Outlook contacts. |
| 5 | **History** tab | Click to display the History fan and the History tab buttons. The History fan displays the associated contacts for all the calls you made and received using the Avaya Equinox for Windows client. Using the History tab buttons, you can view:<br>• all calls you received using the Avaya Equinox for Windows client<br>• all calls you missed while you were using the Avaya Equinox for Windows client<br>• all calls you answered using the Avaya Equinox for Windows client<br>• all calls you made using the Avaya Equinox for Windows client<br>A red badge appears on the History tab to indicate the number of calls you missed since the last time you viewed the History fan. |
| 6 | **IM** tab | Displays the Instant Messaging fan. The Instant Messaging fan displays your instant messaging conversations.<br>When Avaya Multimedia Messaging is selected, the IM fan displays all the Avaya Multimedia Messaging IM conversations. |
| 7 | **Conference** tab | Click to display the Conference fan or roster fan and the Conference tab buttons. The roster fan displays the contact cards for the participants in the conference. The Conference tab buttons enable you to filter the conference participants in the roster fan. Using the Conference tab buttons, you can view:<br>• all participants in the conference<br>• all participants who are viewing the web collaboration session<br>• all participants who dropped from the call<br>You can sort the cards in the Conference fan by most recent conference entry or alphabetically (from A to Z). |
| 8 | Conversation stage | Provides a graphical representation of the selected call. A conversation setup appears for each call you start or join. All calls in progress (active and held) are displayed in the conversation stage.<br>You can use the **New conversation +** button in this area to start a new conversation.<br>You can have a maximum of three conversations at a time. |
| 9 | **Quick dial** field | Allows you to enter a phone number to make a voice or video call. You can also use the dialpad in this field to re-dial a phone number. |

The following figures show the Avaya Equinox for Windows client with the Contacts, History, IM, and Conference tabs expanded. You must be logged in to the Avaya Equinox for Windows client to access these tabs.

Click on the **Contacts** tab to view your list of contacts. You can also hover over a contact, as shown in the image, to access channel buttons for voice call, video call, IM, and additional options.



Avaya Communicator

16135559052

Available

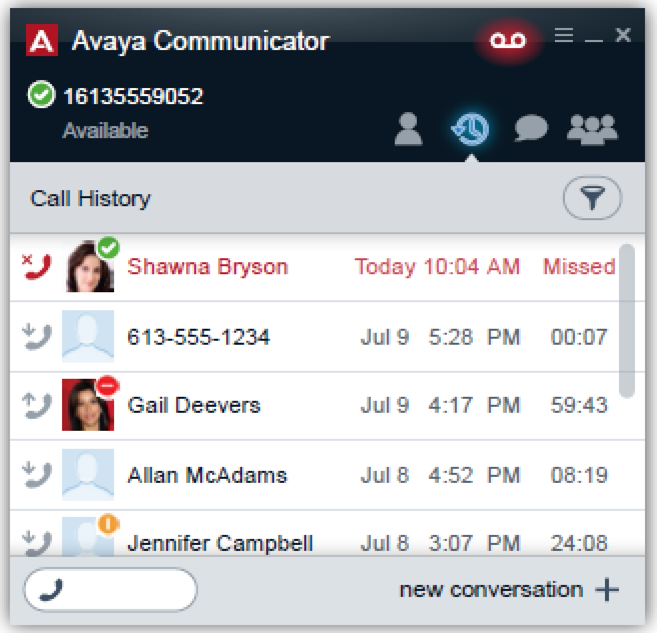
All Contacts ▼

| | |
|---|---|
| Michael Anderson | Offline |
| John Cooperman | Busy |
| William Davis | |
| Elizabeth Mendel | |
| Georgia Nook | Do not disturb |

new conversation +

**Figure 35: Avaya Equinox for Windows with Contacts fan expanded**

Click on the **History** tab to view call history. Missed calls are shown in red.



Avaya Communicator

16135559052

Available

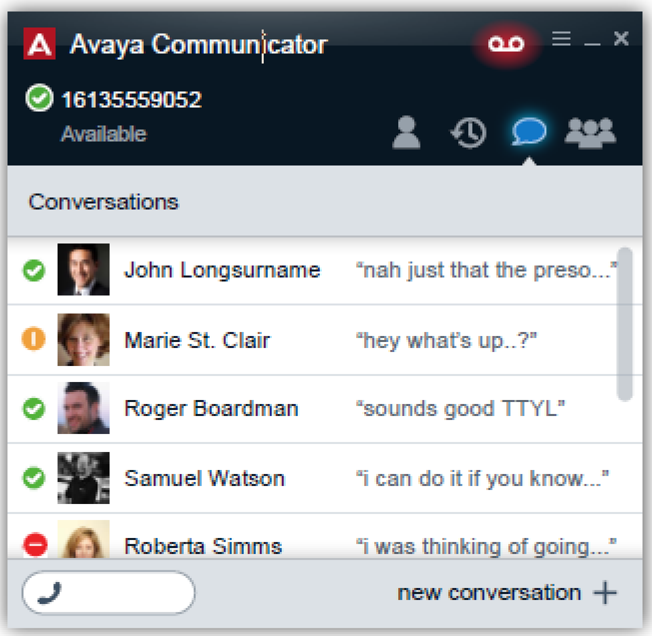
Call History

| | | |
|---|---|---|
| Shawna Bryson | Today 10:04 AM | Missed |
| 613-555-1234 | Jul 9 5:28 PM | 00:07 |
| Gail Deevers | Jul 9 4:17 PM | 59:43 |
| Allan McAdams | Jul 8 4:52 PM | 08:19 |
| Jennifer Campbell | Jul 8 3:07 PM | 24:08 |

new conversation +

**Figure 36: Avaya Equinox for Windows with History fan expanded**

Click on the **IM** tab to view active and missed IM conversations.



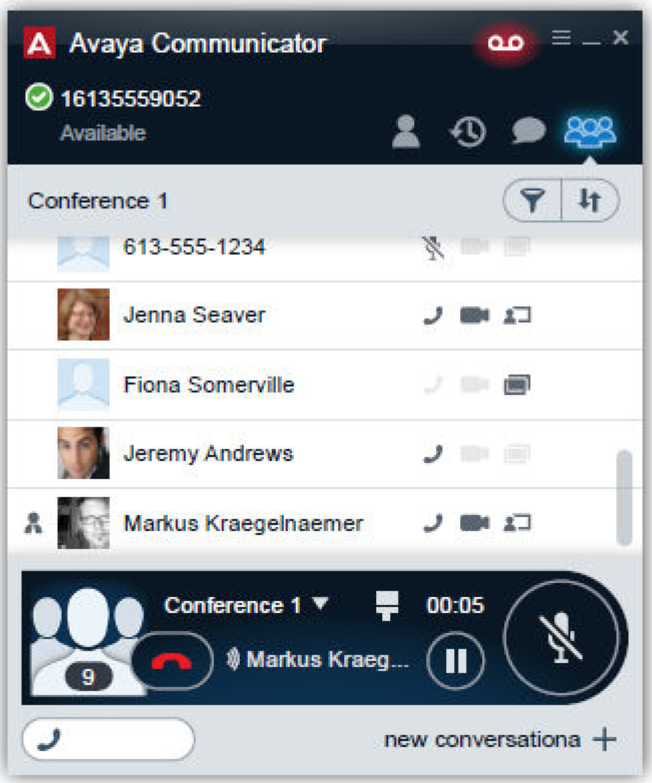
16135559052
Available

Conversations

| | |
|---|---|
| John Longsurname | "nah just that the preso..." |
| Marie St. Clair | "hey what's up..?" |
| Roger Boardman | "sounds good TTYL" |
| Samuel Watson | "i can do it if you know..." |
| Roberta Simms | "i was thinking of going..." |

Figure 37: Avaya Equinox for Windows with Instant Messaging fan expanded

Click on the **Conference** tab to view conference call participants and manage your conference calls.



16135559052
Available

Conference 1

613-555-1234
Jenna Seaver
Fiona Somerville
Jeremy Andrews
Markus Kraegelnaemer

Figure 38: Avaya Equinox for Windows with Conference fan expanded

**Related links**

Overview on page 681

## Button descriptions

The following table shows the main buttons in the Avaya Equinox for Windows client. Buttons are grayed out when unavailable.

| Button | Name | Purpose |
|---|---|---|
| 📞 | **Call** | To make a voice call. |
| 📹 | **Video** | To make a video call. |
| 💬 | **Instant Message** | To send an instant message. |
| ▣ | **Collaboration** | To start or join a Web Collaboration session. |
| ☰ | **Settings** | To open the Settings dialog box where you configure your servers, dialing rules, enterprise directory search settings, contacts search settings, audio settings, video settings, conference settings, messaging, and preferences. The Settings dialog box also displays the software release information and support information.<br>You can also access volume control options from the Settings dialog box. |
| ☎ | **End** | To hang up a voice or video call. |
| 📞 | **Answer** | To answer or join an unanswered active call (bridged, EC500, or Ignored) on the conversation setup stage. |
| × Cancel | **Cancel** | To remove all cards from the conversation setup stage. |

*Table continues…*

| Button | Name | Purpose |
|---|---|---|
| 🔇 | **Mute** | To mute or unmute audio. When the call is muted, the button is blue.<br>⊕ **Tip:**<br>Use the **Mute** functionality in Avaya Equinox. Muting on your desktop or through a headset is reflected on the Avaya Equinox interface. |
| ⣿ | **Dialpad** | To open the dialpad. You can enter touch-tone digits during a call from the dialpad. You can also use the dialpad to enter or re-dial a phone number. |
| ⏸ | **Hold** | To place the current call on hold or resume a call on hold. When the call is on hold, the button is blue. |
| ▼ | **More** | To open the More controls panel, which contains the Moderator controls tab and the Call controls tab. The Moderator controls tab is only available to the moderator. The Call controls tab is available to the moderator and participants of the selected call. |

**Related links**

Overview on page 681

## Multiple Device Access overview

Avaya Equinox supports Multiple Device Access (MDA), which you can use to:

- Log on to the same extension from multiple devices, including mobile EC500 devices.
- Answer a call from multiple devices.
- Join an existing call from other logged in devices.
- Hear simultaneous ringing on all logged in devices when a call is made to your extension.

The Avaya Aura® network configuration, which your administrator configures, determines:

- The number of devices that you can log in to at the same time.
- Whether the first or last logged in device is denied login access when you reach the maximum simultaneous device limit.

For more information, see *Planning for and Administering Avaya Equinox for Android, iOS, Mac, and Windows*.

## MDA limitations

### Support on other devices

- Some devices do not support MDA. You might be able to log in to these devices using the same extension that you used to log in to your Avaya Equinox client. However, other MDA functionality, such as the ability to answer a new call or join an existing call might not work properly.

### Video escalation

- When more than one device is on a call, you cannot escalate the call to video. If additional devices drop from the call and only one device remains on the call, you can escalate that call to a video call.
- When a second device joins a video call, the video screen becomes blank.
- An EC500 device cannot escalate to a video call at any time even if the EC500 device is the only device on the call.

### Joining calls

- If one of the devices on a call is on hold, another device cannot join the call.

### Avaya Aura® Conferencing

- When a second device that is not the Avaya Equinox client joins an existing Avaya Aura® conference, the user of the second device can hear audio on the call. However, the user of the second device cannot access conferencing features or view shared applications. The user of the second device must dial in to the conference separately to access conferencing features.

  If one of the devices on the conference call is the Avaya Equinox client, that device is able to access conferencing features and controls as soon as the other devices drop from the conference call. The Avaya Equinox client does not need to hang up and redial.

# Glossary

**Application Server (AS)**

The application server hosts the Meetme and Adhoc conference applications, and handles the SIP signaling from clients.

**AV MeetMe conference**

A planned Web conference supporting audio and video.

**Avaya Media Server**

The Avaya Media Server hosts conferences and relays media.

**Bandwidth**

Requested bandwidth: This is the bandwidth that is requested at the time of initiating a conference call. This bandwidth request may be negotiated down to a lower bandwidth, or can be thinned by Avaya Aura® Conferencing at some point during the conference.

Negotiated bandwidth: This is a bandwidth that the server allocates to the client and is based on your system configuration and the total available network bandwidth.

Actual bandwidth: This is the bandwidth that is used for a session as determined by the Avaya Aura® Media Server.

**Communication Manager**

A key component of Avaya Aura®. It delivers rich voice and video capabilities and provides a resilient, distributed network for media gateways and analog, digital, and IP-based communication devices. It includes advanced mobility features, built-in conference calling, contact center applications and E911 capabilities.

**Database (DB)**

The database stores configuration information for all Network Elements, such as long and short names, server IP address, and historical OM data.

**Document Conversion Server**

The Document Conversion Server (DCS) is a Linux server that is a document converter and converts PowerPoint, PDF and other document types into formats compatible with Web conferencing.

**Down sessions**

Down sessions are the number of sessions where bandwidth is downgraded because of proactive or reactive thinning.

**Dropped sessions**

Dropped sessions are the number of sessions that dropped by a system due to bandwidth management issues.

**Element Manager (EM)**
Client receives almost all information from the Element Manager using OMI methods. The client sends an OMI request to Element Manager. Element Manager processes this request and determines what to do with it. To get the data for client Element Manager, a request is sent to the database or to other network elements, such as the Application Server or the Web Conferencing Server.

**Gap**
The gap is the difference between the negotiated and actual bandwidth. For example: A request for bandwidth is initiated for a video or audio call (requested bandwidth). The Media Server responds with bandwidth and bandwidth is applied (negotiated bandwidth). Bandwidth continually changes during a call due to factors such as codec, packetization, and time. Therefore, a gap between the actual and negotiated bandwidth occurs.

**Geographic Redundancy**
The capability to implement multiple server instances, such as Session Manager, in geographically distinct data centers.

**Guest**
A guest is an unprovisioned user. The guest has the same privileges as a participant but cannot be promoted to presenter or moderator.

**HPSSA**
Hewlett Packard™ Smart Storage Administrator (HPSSA) is a single interface that sets up, configures, and manages the HP Smart Arrays controllers and the HP SAS Host Bus Adapters (HBA).

**Hybrid Conference**
A hybrid conference includes Web and Audio sessions.

**IPv4**
The fourth revision in the development of IP, and the first version of the protocol to be widely deployed.

**KPI client**
Client receives almost all information from the Element Manager using OMI methods. Usually to get some information client sends an OMI request to Element Manager. Element Manager processes this request and decides what to do with it. To get the data for client Element Manager sends a request to database or to another network elements, such as the Application Server or the Web Collaboration Server.

**License**
There are two types of system licenses: Audio and Video. A unique license is required for each Avaya Aura® Conferencing provisioned user. The License key is installed on the Web License Manager (WebLM) server which is co-resident with System Manager.

**Moderator**
A moderator is a provisioned user and has full control of the conference using either Telephone User Interface (TUI) and User Interface (UI) commands on one of the supported clients.

**Open Management Interface (OMI) call**
SOAP based Web Services provides operations required for Avaya Aura® Conferencing.

**Operator**

An operator controls every aspect of a conference in the same manner as the moderator. An operator does not attend the conference but can be called upon by issuing a Telephony User Interface (TUI) code, if assistance is required.

**Participant**

Participants are people who attend conference calls. A participant can access a conference using an Avaya Aura® Conferencing user account or log in as guest. A participant can be promoted by the moderator to be a presenter or a moderator but cannot change the state of the conference.

**Presenter**

A presenter is a provisioned user. The presenter has the same privileges as a participant but has been promoted to presenter to allow presentation of content using Web collaboration.

**R-factor**

R-factor is a measure of audio quality; the lower the number, the poorer the audio quality. R-factor uses a scale of 0 to 100.

**Session Completion Ratio**

The percentage of rejected sessions compared to the total number of sessions. A session can be rejected for different reason, such as, not enough Bandwidth or not enough licenses.

**Simple Object Access Protocol (SOAP)**

Protocol specification for exchanging structured information in the implementation of Web Services in computer networks.

**Standalone Web conference**

A user starts a standalone Web conference using the Collaboration Agent client before starting an AV MeetMe conference. After an AV MeetMe conference is started, the standalone Web conference is merged with the AV MeetMe conference and is no longer in a standalone state.

**Web Conferencing Server (WCS)**

This server handles user actions and media during Web collaboration.

**Web Service (WS)**

A software system designed to support interoperable machine-to-machine interaction over a network.

# Index