Administering Avaya Aura® Device Services
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, information or the links to third party sites contained within any linked sites. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your 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?detailsId=20059126112456851010 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

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 ACCESES 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 OF 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 THE LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses or 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 thereof. "Designated Processor" means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. ‘Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User through electronic means determined 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. A Named User’s discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

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

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

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

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

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

LICENCED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

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

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

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

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

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

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

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

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

Avaya is a registered trademark of Avaya Inc.

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

## Chapter 1: Introduction
- Purpose............................................................................................................ 9
- Change history................................................................................................. 9

## Chapter 2: Avaya Aura® Device Services overview
- New in this release.......................................................................................... 14
- Architecture topology...................................................................................... 15
- Automatic configuration flow......................................................................... 15
- Components.................................................................................................... 16

## Chapter 3: Management of Avaya Aura® Device Services with the web administration portal
- Logging in to the Avaya Aura® Device Services web administration portal........ 19
- Starting or stopping Avaya Aura® Device Services.......................................... 20
- Managing application sessions........................................................................ 20
  - Application Properties field descriptions..................................................... 20
- Configuring enhanced search options.............................................................. 21
- Enabling an external load balancer................................................................. 21
- Managing certificates in the Avaya Aura® Device Services web administration portal................................................................. 22
  - Managing System Manager certificates...................................................... 22
  - Managing identity certificates..................................................................... 23
  - Managing server interface certificates....................................................... 27
  - Managing truststore certificates................................................................. 27
  - Importing the secure LDAP certificate using the web administration portal.... 28
- Client certificate policy administration............................................................ 28
  - Configuring the client certificate policy using the Avaya Aura® Device Services web administration portal................................................................. 29
- Enabling Avaya Breeze® platform authorization............................................. 31
- Dynamic Configuration service management.................................................. 31
- Messaging server address discovery management.......................................... 31
- LDAP server management................................................................................ 33
  - Configuring the UID mapping attributes when using multiple authentication domains................................................................. 34
  - Adding a new enterprise LDAP server......................................................... 34
  - Administering the LDAP server configuration............................................. 43
  - Modifying enterprise directory attribute mappings...................................... 43
  - Configuring Windows Authentication for Active Directory.......................... 43
  - Modifying the provenance priority................................................................. 45
  - Setting up user synchronization with the LDAP server................................ 45
  - Configuring the internationalization parameters.......................................... 46
  - Adding a trusted host.................................................................................... 47
- Supported characters for LDAP attributes...................................................... 47
Chapter 10: Avaya Aura

Chapter 9: Backup and restore

Chapter 7: AWS-specific management options

Chapter 6: Integrated Windows Authentication administration and management

Chapter 8: Monitoring options

Contents

October 2019 Administering Avaya Aura® Device Services
Comments on this document? infodev@avaya.com

Testing configuration settings................................................................. 79
Publishing the configuration settings.................................................... 80
Viewing published settings................................................................... 81
Retrieving configuration settings for a user.......................................... 82
Import of dynamic configuration settings.............................................. 82
  Importing dynamic configuration settings using a file in the JSON format. 82
  Importing parameter values from a 46xxsettings.txt file.................... 83
  Bulk imports..................................................................................... 83
Administering the default configuration.............................................. 87
Defaults field descriptions................................................................. 87
Split Horizon DNS mapping............................................................... 88
  Mapping the IP address to the FQDN................................................. 89
  Enabling Split Horizon DNS mapping.............................................. 89
  Split Horizon DNS Mapping field descriptions................................. 90

Chapter 6: Integrated Windows Authentication administration and management 91
  Authentication prerequisites............................................................. 91
  Setting up the Windows Domain Controller..................................... 92
    Windows Domain Controller command descriptions...................... 93
  Setting up IWA on the Avaya Aura® Device Services administration portal. 94

Chapter 7: AWS-specific management options.................................. 96
  Updating an existing stack with a new CloudFormation template........ 96

Chapter 8: Monitoring options....................................................... 97
  Monitoring cluster nodes................................................................. 97
    Cluster Nodes field descriptions................................................... 97
  Logs and alarms.............................................................................. 98
    Log management........................................................................... 98
    Monitoring the Avaya Aura® Device Services logs.......................... 98
    Setting up the log level................................................................. 98
    Managing logs.............................................................................. 99
    Alarms......................................................................................... 100
  Enhanced Access Security Gateway for real time support.................... 105
    Enabling the Enhanced Access Security Gateway after Avaya-provided OVA deployment 105
    Removing EASG........................................................................... 106

Chapter 9: Backup and restore......................................................... 107
  Backing up Avaya Aura® Device Services......................................... 107
  Restoring options for standalone and cluster environments.............. 108
    Restoring Avaya Aura® Device Services in a standalone environment 108
    Restoring an Avaya Aura® Device Services cluster........................ 109

Chapter 10: Avaya Aura® Device Services upgrade operations............. 112
  System layer (OS) updates for virtual machines deployed using Avaya-provided OVAs 113
    Determining if a system update is applicable................................ 113
    Downloading, extracting, and staging a system layer update............ 114
    Installing a staged system layer update....................................... 115
Chapter 11: Troubleshooting

DRS fails with constraint error
Checking for DRS synchronization
The AADS.log file contains contact integrity data
ESG cannot connect to Avaya Aura
non-operational
Unable to access the web administration portal when the primary node Session Manager is non-operational.

Upgrading Avaya Aura® Device Services on AVP
Preparing for an AVP upgrade
Upgrading the existing AVP virtual machines
Deploying new AVP virtual machines
Completing the upgrade
Rolling back the AVP upgrade

Upgrading Avaya Aura® Device Services on ESXi or AWS
Creating a full system backup
Upgrading ESXi or AWS virtual machines
Rolling back the ESXi or AWS upgrade
Migrating Utility Server data

Running a patch to allow Avaya Equinox® for Windows to connect to the Web Deployment service
Running a patch to allow the Avaya Aura® Web Gateway to connect to the Avaya Aura® Device Services automatic configuration service
Checking for DRS synchronization

DRS remains in Ready to Repair state
DRS remains in repairing state for a long time
DRS fails with constraint error
Services are not working properly after an installation or upgrade
EASG login using craft username results in an Access Denied error
ESG cannot connect to Avaya Aura® Device Services
A new private key failed to generate
Check for Updates feature is not working
Slow Avaya Aura® Device Services performance

Unable to access the web administration portal when the primary node Session Manager is non-operational
PPM certificate error
Repairing faulty users
Exception in the AADS.log file
The AADS.log file contains contact integrity data
System Manager does not show Avaya Aura® Device Services alarms
Firmware upgrade fails for certain endpoints
Open LDAP replication fails
Open LDAP replication fails if Avaya Aura® Device Services uses a custom identity certificate for server interfaces
Response delay from Open LDAP
Allocating unused disk space to logical volumes
ESXi virtual hardware adjustments
Increasing the virtual disk size of AWS virtual machines
Cannot reinstall a non-seed node due to Cassandra startup error........................................... 147

Chapter 12: Resources.................................................................................................................. 149
  Documentation.......................................................................................................................... 149
    Finding documents on the Avaya Support website.............................................................. 150
    Avaya Documentation Portal navigation............................................................................ 150
  Viewing Avaya Mentor videos................................................................................................. 151
  Support..................................................................................................................................... 152
    Using the Avaya InSite Knowledge Base.............................................................................. 152

Appendix A: Additional administration tools............................................................................ 154
  clitool-acs............................................................................................................................... 155
    Usage example...................................................................................................................... 155
  collectLogs.............................................................................................................................. 156
  statusAADS utility................................................................................................................... 156
  Checking Avaya Aura® Device Services status....................................................................... 157
  Shutting down Avaya Aura® Device Services gracefully....................................................... 157
  System layer commands......................................................................................................... 157
    sys secconfig command........................................................................................................ 158
    sys versions command.......................................................................................................... 159
    sys volmgmt command......................................................................................................... 159
    sys smcvmgmt command...................................................................................................... 163
  Aliases..................................................................................................................................... 166
    app commands...................................................................................................................... 167
    cdto commands..................................................................................................................... 168

Glossary....................................................................................................................................... 169
Chapter 1: Introduction

Purpose

This document describes ongoing administration, management, and maintenance tasks for Avaya Aura® Device Services. Use this document after deploying Avaya Aura® Device Services. For more information about deployment, see Deploying Avaya Aura® Device Services.

Change history

<table>
<thead>
<tr>
<th>Issue</th>
<th>Release Date</th>
<th>Summary of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 7.1.6, Issue 9</td>
<td>October 2019</td>
<td>Updated links.</td>
</tr>
<tr>
<td>Release 7.1.6, Issue 7</td>
<td>April 2019</td>
<td>• Updated <a href="#">New in this release</a> on page 14.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">Avaya Aura Device Services overview</a> on page 14.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added <a href="#">Configuring enhanced search options</a> on page 21.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added <a href="#">Enabling an external load balancer</a> on page 21.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">Enabling Avaya Breeze platform authorization</a> on page 31.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">Messaging server address discovery management</a> on page 31.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">LDAP server management</a> on page 33.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">Adding a new enterprise LDAP server</a> on page 34.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">Enterprise LDAP Server Configuration field descriptions</a> on page 35.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">Modifying the provenance priority</a> on page 45.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">Web Deployment service management</a> on page 53.</td>
</tr>
<tr>
<td>Issue</td>
<td>Release Date</td>
<td>Summary of changes</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added <a href="#">Web Deployment port configuration</a> on page 53.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">Administration of the Dynamic Configuration service</a> on page 72.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">Supported characters for bulk import</a> on page 85.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated sections under <a href="#">Avaya Aura Device Services upgrade operations</a> on page 112.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added sections under <a href="#">System layer (OS) updates for virtual machines deployed using Avaya-provided OVAs</a> on page 113.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added sections under <a href="#">Aliases</a> on page 166.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Minor rephrasing throughout the document.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added <a href="#">Enabling Avaya Breeze platform authorization</a> on page 31.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added <a href="#">Messaging server address discovery management</a> on page 31.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added <a href="#">Updating user attributes in LDAP</a> on page 47.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added <a href="#">Open LDAP user data imports</a> on page 48.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added <a href="#">Structure of a CSV file for the bulk upload procedure</a> on page 49.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added <a href="#">Uploading users in bulk</a> on page 50.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added <a href="#">Changing the PictureURL attribute</a> on page 51.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">Logging in to the Utility Server</a> on page 61.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">Reviewing the disk space occupied by firmware package files</a> on page 61.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">Accessing IP phone custom files</a> on page 64.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">Importing dynamic configuration settings using a file in the JSON format</a> on page 82.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">Integrated Windows Authentication administration and management</a> on page 91.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">Setting up the Windows Domain Controller</a> on page 92.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">Cluster Nodes field descriptions</a> on page 97.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated sections under <a href="#">Backup and restore</a> on page 107.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added a new section: Avaya Aura® Device Services migration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added <a href="#">Response delay from Open LDAP</a> on page 141.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added <a href="#">Cannot reinstall a non-seed node due to Cassandra startup error</a> on page 147.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated <a href="#">Documentation</a> on page 149.</td>
</tr>
<tr>
<td>Issue</td>
<td>Release Date</td>
<td>Summary of changes</td>
</tr>
<tr>
<td>-------</td>
<td>--------------</td>
<td>--------------------</td>
</tr>
</tbody>
</table>
| Release 7.1.3 Service Pack (SP) 1, Issue 5 | August 2018 | • Updated [Setting up a DHCP server](#) on page 60.  
• Updated “Upgrading the existing AVP virtual machines”.  
• Updated “Upgrading ESXi or AWS virtual machines”.  
• Minor reorganization. |
| Release 7.1.3 Service Pack (SP) 1, Issue 4 | July 2018 | • Updated [New in this release](#) on page 14.  
• Updated [Application Properties field descriptions](#) on page 20.  
• Added a new chapter: “Working with the Utility Server”.  
• Updated [Administration of the Dynamic Configuration service](#) on page 72.  
• Updated [Implementation of the dynamic configuration settings](#) on page 74.  
• Added [Assigning a group identifier to a phone model](#) on page 75.  
• Updated [Creating a new configuration](#) on page 75.  
• Updated [Configuration field descriptions](#) on page 76.  
• Updated [Avaya Aura Device Services specific parameters](#) on page 78.  
• Updated [Overwriting an existing configuration](#) on page 79.  
• Updated [Publishing the configuration settings](#) on page 80.  
• Updated [Viewing published settings](#) on page 81.  
• Updated [Bulk imports](#) on page 83.  
• Updated [Administrating the default configuration](#) on page 87.  
• Updated [Split Horizon DNS mapping](#) on page 88.  
• Updated the sections under [ESXi virtual hardware adjustments](#) on page 144.  
• Added “Adjusting resources within the virtual machine”.  
• Updated the sections under “Backup and restore operations”.  
• Updated the sections under [Avaya Aura Device Services upgrade operations](#) on page 112.  
• Added “Test configurations for the Dynamic Configuration feature do not work after rollback”.  
• Added [Firmware upgrade fails for certain endpoints](#) on page 140.  
• Updated [Documentation](#) on page 149. |
| Release 7.1.3, Issue 3 | June 2018 | • Added a new section: [System layer commands](#) on page 157.  
• Reorganized dynamic configuration information.  
• Consolidated procedures that are performed in the web administration portal. |
<table>
<thead>
<tr>
<th>Issue</th>
<th>Release Date</th>
<th>Summary of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Release 7.1.2, Issue 2</td>
<td>December 2017</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated Administration of the Dynamic Configuration service on page 72.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated “Upgrading Avaya Aura® Device Services”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added a new field, Use Additional Base Context DN. See Enterprise LDAP Server Configuration field descriptions on page 35.</td>
</tr>
<tr>
<td>Issue</td>
<td>Release Date</td>
<td>Summary of changes</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Release 7.1, Issue 1</td>
<td>July 2017</td>
<td>• Added <a href="#">Configuring additional base context DNs</a> on page 42.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added migration information for Avaya Aura® Device Services Release 7.1.2 in the sections under “Avaya Aura® Device Services migration to Release 7.1.2”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added <a href="#">AWS-specific management options</a> on page 96.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added <a href="#">Repairing faulty users</a> on page 137.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added information on managing logs, see <a href="#">Managing logs</a> on page 99.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated information on administration tools. See <a href="#">Additional administration tools</a> on page 154.</td>
</tr>
</tbody>
</table>
Chapter 2: Avaya Aura® Device Services overview

With Avaya Aura® Device Services, you can roll out multiple clients and seamlessly transition between devices. Avaya Aura® Device Services acts as a single point of administration for endpoints, and it can also provide file server capabilities, such as providing firmware and settings files. Avaya Aura® Device Services can handle traditional IP phones, such as the 96xx Series Phones, and the complex configuration of SIP endpoints, such as Avaya Equinox®.

SIP endpoints, such as Avaya Equinox®, integrate telephony, video, chat, email, and presence. To log in to and use all these services, the device must be configured with multiple FQDNs or IP addresses, login IDs, and passwords. Once logged in, you require the appropriately formatted contact address to initiate communication, and Avaya Aura® Device Services can provide this.

Avaya Equinox® also provides BYOD capabilities, which allow users to use their own devices. Each device has different capabilities, so the appropriate settings must be pushed to each device. Using the Dynamic Configuration service, Avaya Aura® Device Services provides dynamically created setting files that include system-wide parameters, user-specific parameters, and device-specific parameters.

As an administrator, you must maintain software-based soft clients on a limited set of versions to ensure consistent feature sets and security. With hard phones, such as 96xx Series Phones, you can initiate a firmware download by forcing the phone to reboot. With a soft phone, such as Avaya Equinox®, you cannot manually force the software to update unless it is configured through Avaya Aura® Device Services.

New in this release

The following is a summary of new functionality that has been added to Avaya Aura® Device Services Release 7.1.6.

Enhanced search

Avaya Aura® Device Services now supports enhanced search, which enables Avaya Equinox® client users to search by name, location, or department. You can configure the department search capability in the Avaya Aura® Device Services web administration portal.

Contact groups

As of Release 3.6, Avaya Equinox® client users can create contact groups and sort their contacts into the appropriate groups. This functionality is managed using Avaya Aura® Device Services API. For general information about APIs, see Avaya DevConnect.
Avaya Breeze® platform authorization

Users that previously authenticated using the Avaya Breeze® platform Authorization application can now use single sign-on (SSO) capabilities for Avaya Aura® Device Services.

Architecture topology

The following diagram shows the Avaya Aura® Device Services architecture:

Avaya Aura® Device Services is aligned with Session Manager, Appliance Virtualization Platform, and the VMware virtualized environment. The VMware license embedded in the Appliance Virtualization Platform does not support vCenter.

Automatic configuration flow

The following diagram shows the automatic client configuration flow.
Components

The following table lists key components that interwork with Avaya Aura® Device Services. For more information about interoperability and supported product versions, see https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml?name=Avaya+Aura+Device+Services.
**Components**

<table>
<thead>
<tr>
<th>Components</th>
<th>Description</th>
</tr>
</thead>
</table>
| Avaya Aura® core | Avaya Aura® Device Services requires the following Avaya Aura® key components:  
  • System Manager: For centralized management. System Manager also enables other capabilities, including licensing with Avaya WebLM.  
  • Session Manager: For registration and telephony functions, such as call escalation.  
  • Communication Manager: For organizing and routing voice, data, image, and video transmissions.  
  • Presence Services: For Presence and IM functionality. |
| Avaya Aura® Session Border Controller (Avaya SBCE) | Avaya SBCE provides a common element to enable secure access to the Avaya infrastructure from untrusted networks, such as the internet. In addition to SIP firewall services, this component provides the Reverse Proxy services required for HTTP signaling, media traversal, and access to other data services. |
| Enterprise Directory | The corporate LDAP server. For example: Microsoft Active Directory. |

**Virtualized components**

<table>
<thead>
<tr>
<th>Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi Host</td>
<td>A virtual machine running the ESXi Hypervisor software.</td>
</tr>
<tr>
<td>ESXi Hypervisor</td>
<td>A platform that runs multiple operating systems on a host computer at the same time.</td>
</tr>
<tr>
<td>vSphere Client</td>
<td>An application that installs and manages virtual machines. vSphere Client connects to a vCenter server or directly to an ESXi host if a vCenter Server is not used. The application is installed on a personal computer or accessible through a web interface.</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>An administrative interface from VMware for the entire virtual infrastructure or data center, including VMs, ESXi hosts, deployment profiles, distributed virtual networking, and hardware monitoring.</td>
</tr>
<tr>
<td>Appliance Virtualization Platform</td>
<td>A platform that is a customized OEM version of VMware ESXi. With Appliance Virtualization Platform, customers can run any combination of supported applications on Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements. Appliance Virtualization Platform is available only in an Avaya-appliance offer. Avaya-appliance offer does not support VMware® tools, such as vCenter and vSphere Client. You can configure and manage Appliance Virtualization Platform by using Solution Deployment Manager that is part of System Manager, or by installing the Solution Deployment Manager client.</td>
</tr>
<tr>
<td>Solution Deployment Manager</td>
<td>The centralized software management solution of Avaya that provides deployment, upgrade, migration, and update capabilities for the Avaya Aura® virtual applications.</td>
</tr>
</tbody>
</table>
Virtualized components | Description
--------------------------|--------------------------------------------------
Open Virtualization Appliance | The virtualized operating system and application packaged in a single file that is used to deploy a virtual machine.

You can deploy Avaya Aura® Device Services if you have any of the following:

- Solution Deployment Manager
- vSphere Client
- vCenter server
- Appliance Virtualization Platform
Chapter 3: Management of Avaya Aura® Device Services with the web administration portal

Logging in to the Avaya Aura® Device Services web administration portal

About this task
You can access the Avaya Aura® Device Services web administration portal by using the Avaya Aura® Device Services URL or System Manager. To use System Manager for single sign on, you must add the Avaya Aura® Device Services instance to System Manager.

Procedure
1. Open the web browser.
2. Type the URL in one of the following formats:
   - https://<IP_Address>:8445/admin/
   - https://<FQDN>:8445/admin/
   In the DNS, add an entry to map IP address with the FQDN.
   If the FQDN does not resolve through DNS, you must add the Avaya Aura® Device Services IP address and FQDN in the hosts file of the system from which you are accessing the Avaya Aura® Device Services web administration portal. The default path of the hosts file on a Microsoft Windows system is C:\Windows\System32\drivers \etc\hosts.
3. Press Enter.
   If your browser does not have a valid security certificate, the system displays a warning with instructions to load the security certificate.
4. (Optional) If you are certain your connection is secure, accept the server security certificate to access the Login screen.
5. On the Login screen, enter your user name and password.
   To access the web-based administration portal, use an account with an administrator role defined in the LDAP server configuration.
6. Click Log on.

---

### Starting or stopping Avaya Aura® Device Services

**Procedure**

1. On the Avaya Aura® Device Services web administration portal, navigate to Service Control > Application Management.

2. Select the Device Services check box and then do one of the following:
   a. Click Start to start Avaya Aura® Device Services.
   b. Click Stop to stop Avaya Aura® Device Services.

---

### Managing application sessions

**About this task**

Use this procedure to:

- Set a timeout period for terminating inactive, idle, or unattended sessions.
- Manage concurrent HTTP sessions.

**Procedure**

1. On the Avaya Multimedia Messaging web administration portal, navigate to Service Control > Application Management.

2. In the Application Properties area, complete the required settings, which are described in Application Properties field descriptions on page 20.

3. Click Save.

---

### Application Properties field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Admin HTTPSession Timeout (minutes)      | The timeout period for the Avaya Aura® Device Services web administration portal.  
                                          | You can enter a value between 1 and 60 minutes. The default value is 15 minutes. |
| Application HTTPSession Timeout (minutes)| The timeout period for application components.  
<pre><code>                                      | You can enter a value between 1 and 60 minutes. The default value is 15 minutes. |
</code></pre>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximum Concurrent HTTP Sessions</strong></td>
<td>The maximum number of active sessions that are available for application components. If the number of sessions exceeds the configured value for any component, a 503 error, which indicates that service is unavailable, is generated by that component. You can enter a value between 100 and 1,000,000. The default value is 200,000.</td>
</tr>
<tr>
<td><strong>Concurrent HTTP Sessions per User</strong></td>
<td>The number of active sessions that are available per user. If the number of sessions exceeds the configured value for any user, a 429 error, which indicates that there are too many requests, is sent as a response to the user's request. You can enter a value between 10 and 1000. The default value is 50.</td>
</tr>
</tbody>
</table>

### Configuring enhanced search options

**About this task**

The enhanced search feature enables Avaya Equinox® client users to search by name, location, or department. Use this procedure to configure the department search capability in the Avaya Aura® Device Services web administration portal.

**Procedure**

1. On the Avaya Aura® Device Services web administration portal, navigate to **Client Administration > Enhanced Search Configuration**.
2. From the **Department** drop-down list, select one of the following options:
   - **startsWith**: Searches for department names that start with the search text entered. The relevant users from the departments are displayed.
   - **contains**: Searches for deployment names that contain the search text entered. The relevant users from the department are displayed.
3. Click **Save**.

### Enabling an external load balancer

**About this task**

Use this procedure to enable an external load balancer. When you enable the external load balancer, the internal load balancer is disabled.
Before you begin

- Configure the external load balancer. For more information about the external load balancer requirements and configuration options, see “External load balancer requirements” and “Port configuration for an external load balancer” in *Deploying Avaya Aura® Device Services*.
- Disable the virtual IP on all nodes.
- Set the Avaya Aura® Device Services front-end FQDN to the FQDN of the external load balancer on all nodes.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to External Access > Load Balancer Check.
2. Select the Enable use of an external load balancer check box.
3. Click Save.

Managing certificates in the Avaya Aura® Device Services web administration portal

About this task

You can use the Avaya Aura® Device Services administration portal to review and manage certificates. The management options in the administration portal do not replace the setup that you need to complete during installation. After installation is completed, use the web administration portal for management when possible. Only use the configuration utility if the administration portal is not available or for troubleshooting purposes.

Before you begin

- You must have the Security Administrator role to access certificate management options. For more information, see the “LDAP configuration” section in *Deploying Avaya Aura® Device Services*.
- In a cluster environment, ensure that all nodes in the cluster are running.

Procedure

1. On the Avaya Aura® Device Services web administration portal, click Certificate Management.
2. Click the appropriate tab.

   The procedures below describe the tasks you can perform on each tab.

Managing System Manager certificates

About this task

Use this procedure to manage System Manager security identity certificates.
Managing certificates in the Avaya Aura® Device Services web administration portal

Procedure

1. Click the **SMGR Certificates** tab.

   The **System Manager Address**, **System Manager HTTPS Port**, and **Common Name** fields are automatically populated and cannot be modified from the Avaya Aura® Device Services web administration portal. You can use the Avaya Aura® Device Services configuration utility to modify this information if required. The configuration utility is described in *Deploying Avaya Aura® Device Services*.

2. In the **Node Address** drop-down menu, do one of the following to generate a certificate:
   - Choose a node for a cluster configuration.
     
     If you choose the **All Cluster Nodes** option, certificates will be generated automatically for all cluster nodes.
   - Keep the default setting for a standalone configuration.

3. In **System Manager Enrollment Password**, type the enrollment password as defined on the System Manager web console.

4. Click **Generate Certificates** to start requesting certificates from System Manager.

5. Restart the Avaya Aura® Device Services after the certificates are generated.

This completes all the certificate updates. For cluster environment, only the remote node is restarted.

---

Managing identity certificates

**Procedure**

1. Click the **Identity Certificates** tab.

2. Use the following subsections to manage CSRs, keystore data, and server identity certificates.

3. After performing the required task, when prompted, restart the Avaya Aura® Device Services server for the changes to take effect.

Managing CSRs

**Procedure**

In the Certificate Signing Requests area, do one of the following:

- To set up a new CSR, click **Create** and then follow the steps in *Creating CSRs* on page 24.
- To remove an existing CSR, select it and then click **Delete**.
- To process a signed CSR, click **Process Signing Request**. For more information, see *Processing CA signing requests* on page 26.
Creating CSRs

About this task
This procedure provides a high-level overview of how to create CSRs.

Procedure
1. If you clicked Create in the Certificate Signing Requests area, complete the following settings in the Create Certificate Signing dialog box and then click Apply.
   a. In Alias, type an alias using alphanumeric characters.
      An example of an alias is ottawacrt123.
   b. Complete the other settings as required.
      You can use the Show Advanced Settings button to view additional settings information. For more information about settings, see Create Certificate Signing Request screen field descriptions on page 25.
2. Ensure that the CSR file is successfully saved on your computer.
   The generated CSR is also added to the Certificate Signing Requests area.
   In a cluster configuration, the CSR list on all nodes is identical.
3. (Optional) In a cluster environment, if the CSR is not available on a node, click Propagate to synchronize requests from the current node to the cluster.

Next steps
Provide the CSR file to the CA for signing and apply the signed CSR as described in Processing CA signing requests on page 26.

Creating a CSR for a certificate to connect Avaya Aura® Device Services to the Avaya Aura® Web Gateway

About this task
If you are planning to connect Avaya Aura® Device Services to the Avaya Aura® Web Gateway, you need to use a certificate containing information about the FQDN that is used for server-to-server communication. Otherwise, this FQDN will not be part of the SAN, and Avaya Aura® Device Services will not connect to the Avaya Aura® Web Gateway.

Before you begin
• When deploying a CloudFormation stack, provide the host name that is mapped directly to the Avaya Aura® Device Services nodes in the Hostname for server-to-server field. For more information, see “Amazon Web Services deployments” in Deploying Avaya Aura® Device Services.

Procedure
2. In the Certificate Signing Requests area, click Create.
3. In the Create Certificate Signing Request window, click Show Advanced Settings.
4. Select **Specify SAN Manually**.

5. Select **Add FQDN** and provide the following SANs:
   - Load Balancer FQDN.
   - FQDN that is used for server-to-server communication.
   - FQDNs of all nodes in the cluster.

For example, an Avaya Aura® Device Services cluster with three nodes uses `aads` for the stack name and `aadsrv` for the server-to-server communication host name. The domain is `aadsrv.ca.avaya.com`. In this case, the CSR must contain the following SANs:

- `aads.ca.avaya.com` for the load balancer.
- `aadsrv.ca.avaya.com` for server-to-server communication.
- `aads0.ca.avaya.com` for the first node in the cluster.
- `aads1.ca.avaya.com` for the second node in the cluster.
- `aads2.ca.avaya.com` for the third node in the cluster.

**Next steps**

1. Provide the CSR file to the System Manager CA and apply the signed CSR as described in [Processing CA signing requests](#) on page 26.

2. Assign the signed certificate to the Internal server interface as described in [Managing server interface certificates](#) on page 27.

**Create Certificate Signing Request screen field descriptions**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>The name of the certificate</td>
</tr>
<tr>
<td>Common Name</td>
<td>The FQDN of the node. For example, <code>amm.example.com</code></td>
</tr>
<tr>
<td></td>
<td>You cannot provide wildcard (*) characters in this field.</td>
</tr>
<tr>
<td>Use Existing FQDNs for SAN</td>
<td>Use this option to select a particular node in a cluster for which a certificate should be generated. You can also select all cluster nodes.</td>
</tr>
<tr>
<td>Specify SAN manually</td>
<td>Use this option to manually specify additional FQDNs or IP addresses for which the certificate should be generated.</td>
</tr>
<tr>
<td>Subject Alternative Name</td>
<td>An optional text field that can be used to further identify this certificate.</td>
</tr>
<tr>
<td></td>
<td>You can provide multiple entries in this field. You cannot provide wildcard (*) characters in this field.</td>
</tr>
<tr>
<td>Key Bit Length</td>
<td>The certificate key length in bits.</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>The hash algorithms to be used with the RSA signature algorithm.</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>The group within the company or organization creating the certificate.</td>
</tr>
<tr>
<td>Organization</td>
<td>The name of the company or organization creating the certificate.</td>
</tr>
<tr>
<td>City/Locality Name</td>
<td>The city where the certificate is being created.</td>
</tr>
<tr>
<td>State/Province Name</td>
<td>The state/province where the certificate is being created.</td>
</tr>
</tbody>
</table>
### Processing CA signing requests

**Procedure**

1. Use the appropriate CA documentation to sign the signing request with the CA.
2. In the Certificate Signing Request area, select the appropriate signing request and then click **Process Signing Requests**.
3. In the Process Signing Request dialog box, click **Choose file** to add the signed certificate and then click **Apply**.

**Result**

The signed certificate is removed from the Certificate Signing Requests area and added to the Keystore area.

### Managing keystore data

**Procedure**

In the Keystore area, do one of the following:

- To import keystore data, click **Import** and then perform **Importing keystore data** on page 26.
- To export a certificate in the PKCS12 format, select a keystore file and then click **Export**.
  
  In the Export Certificate dialog box, you can enter a password to protect your exported file.
- To view details about a keystore file, click **Details**.
- To remove an existing keystore file, select it and then click **Delete**.

**Importing keystore data**

**Procedure**

If you clicked **Import**, complete the following settings in the Import Certificate dialog box and then click **Apply**.

1. In the **Certificate Type** drop-down menu, select a format for importing the certificate.
2. From **Certificate File**, click **Choose file** to add the certificate file in the selected format.
3. If you selected the PEM format, in **Key File**, click **Choose file** to add the key file in the PEM format.
4. If you selected the PKCS12 format, in **Password**, type the password for the imported certificate.
5. In **Alias**, type an alias to be used for the imported certificate.
Managing server interface certificates

Procedure

1. Navigate to the Server Interfaces area.
2. In a cluster environment, select the node to administer from the Node Address list.
3. Do one of the following:
   • To assign the certificate to a specific server interface, click Assign and then complete the settings in the Assign Certificates dialog box as described in Certificate assignment descriptions on page 27.
     
     If the certificate was assigned only to a selected node, then services on that node need to be restarted to apply the change. If the assignment applies to an entire cluster, then you must restart all nodes in the cluster.
   • To view details about the certificate, click Details.
   • To export the certificate in the PKCS12 format, click Export.

Certificate assignment descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Specifies the interface for REST API to the clients.</td>
</tr>
<tr>
<td>Internal</td>
<td>Specifies the interface being used for server-to-server component communication.</td>
</tr>
<tr>
<td>OAM</td>
<td>Specifies the Operations, Administration, and Maintenance (OAM) interface.</td>
</tr>
</tbody>
</table>

Managing truststore certificates

About this task

Use this procedure to manage truststore certificates available on Avaya Aura® Device Services.

Procedure

1. Click the Truststore tab.
2. In the Truststore area, choose a certificate and click one of the following:
   • Import: To import a certificate in PEM or PKCS12 format.
   • Details: To view information about the certificate.
   • Delete: To delete the certificate from the truststore.
   • Export: To export the certificate in the PEM format.
3. Restart Avaya Aura® Device Services after importing or deleting certificates for changes to take effect. For cluster environment, restart all the nodes in the cluster for changes to take effect.

---

**Importing the secure LDAP certificate using the web administration portal**

**About this task**

For secure connectivity to LDAP servers, you must import an LDAP certificate file to the Tomcat trust store. The following procedure describes how to import the LDAP certificate using the Avaya Aura® Device Services web administration portal.

**Before you begin**

Ensure that the FQDN that is configured as the address of the LDAP source is defined in one of the following places:

- The Common Name in the Subject field.
- Subject Alternative Name.

You can use the following `openssl` command in the Avaya Aura® Device Services CLI to verify the certificate content:

```
openssl s_client -connect <ldap server:port> | openssl x509 -noout -text
```

**Procedure**

1. On the Avaya Aura® Device Services web administration portal, navigate to Server Connections > LDAP Configuration > Enterprise Directory.
2. Select the Secure LDAP check box.
3. Click Import Certificate.
4. In the Import Certificate window, click Choose File and select the certificate from your local system.
5. Click Save.

   The system uploads the certificate to a secure LDAP Server. If a certificate is already uploaded, the system overwrites the existing certificate.

---

**Client certificate policy administration**

You can configure client certificates to establish a secure connection. As per your requirement, you can choose how the server validates certificates for Avaya Aura® Device Services clients. Changing the certificate setting might affect the client's ability to connect to Avaya Aura® Device Services.
Configuring the client certificate policy using the Avaya Aura® Device Services web administration portal

About this task
You can configure client certificates to establish a secure connection. As per your requirement, you can choose how the server validates certificates for Avaya Aura® Device Services clients. Changing the certificate setting might affect the client’s ability to connect to Avaya Aura® Device Services.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to Client Administration > HTTP Clients.

   The system displays the Client-Device Certificate Policy page.

2. To set the client certificate policy for the REST request, in the REST field, select the appropriate setting.

   Note:
   If the client certificate policy for an interface is set to OPTIONAL, OPTIONAL_NO_CA, or REQUIRED client certificates, when presented to the client:
   • Must have digitalSignature key usage if key usage information is present.
   • Must have id-kp-clientAuth if extended key usage is present. This is the TLS WWW client authentication extended key usage.

   If the certificate does not have key usage information, the certificate allows all key usages.

3. To set the client certificate policy for the administrator UI (OAMP), in the OAMP field, select the appropriate setting.

4. Click Save.

Client-Device Certificate Policy field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>REST</td>
<td>Specifies certificate processing options for REST requests. The options are:</td>
</tr>
<tr>
<td></td>
<td>• NONE: The server does not check for a certificate. The connection is established with or without a valid certificate.</td>
</tr>
<tr>
<td></td>
<td>• OPTIONAL: The server requests a certificate. The connection is established with or without a certificate, but the process stops if a client</td>
</tr>
</tbody>
</table>
provides an invalid or untrusted certificate, and the system returns the error code HTTP 400.

- **OPTIONAL_NO_CA**: The server requests a certificate. The connection is established with any valid certificate even if CA is untrusted, but the process stops if a client provides an invalid certificate, and the system returns the error code HTTP 400.

- **REQUIRED**: The server requests a certificate. The server rejects a connection if a client fails to provide a valid certificate, and the system returns the error code HTTP 400.

The default value is: **OPTIONAL**.

**OAMP**

- Specifies certificate processing options for OAMP.

  The options are:

  - **NONE**: The server does not check for a certificate. The connection is established with or without a valid certificate.

  - **OPTIONAL**: The server requests a certificate. The connection is established with or without a certificate, but the process stops if a client provides an invalid or untrusted certificate, and the system returns the error code HTTP 400.

  - **OPTIONAL_NO_CA**: The server requests a certificate. The connection is established with any valid certificate even if the CA is untrusted, but the process stops if a client provides an invalid certificate, and the system returns the error code HTTP 400.

  - **REQUIRED**: The server requests a certificate. The server rejects a connection if a client fails to provide a valid certificate, and the system returns the error code HTTP 400.

  The default value is: **OPTIONAL**.

---

**Button** | **Description**
---|---
Save | Saves the changes made to the settings.
Cancel | Ignores your changes and resets the settings to default values.
Enabling Avaya Breeze® platform authorization

About this task
Use this procedure to enable single sign-on (SSO) capabilities for Avaya Aura® Device Services users that previously authenticated using the Avaya Breeze® platform Authorization application.

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

For more information about Authorization Service, see “Authorization Service” in Administering Avaya Breeze® platform.

Before you begin
Obtain the Avaya Breeze® platform authorization certificate file in the .PEM format. For more information, see Administering Avaya Breeze® platform.

Procedure
2. Click Choose File and select the .PEM file that you exported from the Avaya Breeze® platform node.
3. Click Save.

Dynamic Configuration service management
With the Dynamic Configuration service, the system can dynamically retrieve and deploy the device configuration settings to the Avaya Equinox® clients. For more information about the Dynamic Configuration service, see the sections under Administration of the Dynamic Configuration service on page 72.

Messaging server address discovery management
Avaya Aura® Device Services provides clients with the Presence Services or Avaya Multimedia Messaging server FQDN and port values using the ESMSRVR and ESMPORT parameters respectively. When clients receive a server FQDN, they resolve it to a single IP address and then try to connect to this address. Previously, Avaya Aura® Device Services used System Manager user profiles as the primary source for server FQDN values.

If the server FQDN resolves to multiple FQDN addresses, there might be an issue when clients resolve the FQDN and try to connect to a failed IP address, but do not try to use other IP addresses. To prevent this issue, as of Release 7.1.5, Avaya Aura® Device Services can perform
automatic DNS SRV service lookup to resolve the server FQDN and port. Avaya Aura® Device Services sets the values of ESMSRVR and ESMPORT based on the first matching record it finds during the DNS SRV query.

Avaya Aura® Device Services supports the following discovering methods for the messaging server FQDN value:

1. Publishing the ESMSRVR and ESMPORT values using the Dynamic Configuration service.
2. Obtaining the FQDN value from the System Manager user profile. This method can be enabled or disabled using the legacy ESM_MULTISITE_ENABLED parameter.
3. Performing DNS SRV service lookup on the FQDN that is found in the System Manager user profile. This method can be enabled using the new AUTO_AMM_LOOKUP_ENABLED parameter.

By default, automatic DNS lookup is disabled, so Avaya Aura® Device Services uses server FQDN and port values that are configured in the System Manager user profile. If you want to resolve the server FQDN using DNS SRV lookup, you must set the AUTO_AMM_LOOKUP_ENABLED parameter to 1 using the Dynamic Configuration service.

In a migration scenario, the system continues to use the values configured before migration. In this case, automatic DNS lookup is enabled only if ESM_MULTISITE_ENABLED was set to 0 before migration.

The following table shows which ESMSRVR and ESMPORT values Avaya Aura® Device Services provides to clients depending on the ESM_MULTISITE_ENABLED and AUTO_AMM_LOOKUP_ENABLED values.

<table>
<thead>
<tr>
<th>Dynamic Configuration parameter value</th>
<th>Value Avaya Aura® Device Services provides to clients</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ESM_MULTISITE_ENABLED</strong></td>
<td><strong>AUTO_AMM_LOOKUP_ENABLED</strong></td>
</tr>
<tr>
<td>1</td>
<td>Not published. Derived value is 0</td>
</tr>
<tr>
<td>0</td>
<td>Not published. Derived value is 1</td>
</tr>
<tr>
<td>Not published. Derived value is 1</td>
<td>Not published. Derived value is 0</td>
</tr>
</tbody>
</table>
Dynamic Configuration parameter value | Value Avaya Aura® Device Services provides to clients
---|---
| ESM_MULTISITE_ENABLED | AUTO_AMM_LOOKUP_ENABLED | ESMSRVR | ESMPORT |
1 | 0 | The value configured in the System Manager user profile. If the value is not found, then the published ESMSRVR value is used, if available. | The ESMPORT value published using the Dynamic Configuration service is used, if available. |
1 | 1 | The value received using the DNS SRV query. If the query fails or no result is found, then the published ESMSRVR value is used, if available. | The value received using the DNS SRV query. If the query fails or no result is found, then the published ESMPORT value is used, if available. |
0 | 1 | The value received using the DNS SRV query. If the query fails or no result is found, then the published ESMSRVR value is used, if available. | The value received using the DNS SRV query. If the query fails or no result is found, then the published ESMPORT value is used, if available. |
0 | 0 | The ESMSRVR value published using the Dynamic Configuration service is used, if available. | The ESMPORT value published using the Dynamic Configuration service is used, if available. |

When the DNS SRV query fails, Avaya Aura® Device Services assumes that no matching DNS records were found. Avaya Aura® Device Services then uses ESMSRVR and ESMPORT values that are set according to the rules listed in the table.

**LDAP server management**

You must configure the enterprise LDAP server to authenticate the users and administrators of Avaya Aura® Device Services. When you log in to the Avaya Aura® Device Services web administration portal, the system displays the enterprise LDAP server that you configure at the time of Avaya Aura® Device Services deployment.

**Important:**

- For secure connectivity to LDAP servers, you must import an LDAP certificate file to the Tomcat trust store. For more information, see [Importing the secure LDAP certificate using the web administration portal](#) on page 28.
- After creating a new user or updating the details in System Manager, you must force LDAP synchronization or wait 24 hours for your changes to take effect.
Configuring the UID mapping attributes when using multiple authentication domains

About this task

If you are using multiple authentication domains, the UID mapping attribute value set for each LDAP server must be domain-qualified. Therefore, the value must include the @domain part. The following values are supported:

- mail
- userPrincipalName
- Any custom attribute that uses a domain-qualified value.

Note:

If you are not using multiple authentication domains, Avaya Aura® Device Services supports only the following values for the UID mapping attribute:

- uid, if you are using Open LDAP.
- sAMAccountName
- mail
- userPrincipalName

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to Server Connections > LDAP Configuration > Enterprise Directory.
   The system displays the Enterprise LDAP Server Configuration page.
2. For each LDAP server in the system, in the UID Attribute ID field, enter the appropriate value.

Adding a new enterprise LDAP server

About this task

Use this procedure to add a new LDAP server to Avaya Aura® Device Services.

After you have added a server, you cannot modify the server URL or remove the LDAP data source.

Before you begin

If you are planning to use multiple authentication domains, configure the UID mapping attributes as specified in Configuring the UID mapping attributes when using multiple authentication domains on page 34.
Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to Server Connections > LDAP Configuration > Enterprise Directory.

   The system displays the Enterprise LDAP Server Configuration page.

2. Click the plus (+) icon.

   The system displays the New Directory tab.

3. In the Enterprise-Directory Type field, click the LDAP server directory that you want to add.

4. In the Provenance Priority field, type the priority of the enterprise LDAP server directory.

5. In the Server Address and Credentials section, specify the parameters of the enterprise LDAP server directory.

   For more information about attributes, see Enterprise LDAP Server Configuration field descriptions on page 35.

6. If you want to use the new server for authentication and authorization, do the following:
   a. Select the Use for Authentication check box.
   b. Configure role-related attributes, such as Role Filter, Role Attribute ID, and Role Context DN.

7. Click Save.

Enterprise LDAP Server Configuration field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise-Directory Type</td>
<td>Specifies the name of the enterprise directory. The options are:</td>
</tr>
<tr>
<td></td>
<td>• ActiveDirectory_2008</td>
</tr>
<tr>
<td></td>
<td>• ActiveDirectory_2012</td>
</tr>
<tr>
<td></td>
<td>• ActiveDirectory_2016</td>
</tr>
<tr>
<td></td>
<td>• Novell 8.8</td>
</tr>
<tr>
<td></td>
<td>• Domino 7.0 or 8.5.3</td>
</tr>
<tr>
<td></td>
<td>• LDS_2008</td>
</tr>
<tr>
<td></td>
<td>• LDS_2012</td>
</tr>
<tr>
<td></td>
<td>• OpenLDAP 2.4.44</td>
</tr>
<tr>
<td></td>
<td>• OracleDirectoryServer 11.1.1</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Provenance Priority</td>
<td>Specifies the provenance priority of the enterprise directory. Provenance priority is used while merging contacts. If a value is available in more than one directory, the value in the directory with higher provenance priority is returned. For example, if firstName is obtained from two directories, the firstName from the source with higher provenance priority is returned. You can assign a value between 2 to 10. You cannot assign Provenance priority 1 because it is always assigned to the authorization directory. Provenance priority 1 is the highest and 10 is the lowest. Provenance priority must be different for each enterprise directory or source.</td>
</tr>
</tbody>
</table>

### Server Address and Credentials

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure LDAP</td>
<td>Indicates whether the LDAP server connection is secure or not. If you are using a secure LDAP connection, you must also import the LDAP server trusted certificate to Avaya Aura® Device Services.</td>
</tr>
<tr>
<td>Import Certificate</td>
<td>Specifies the LDAP server trusted certificate. This field is mandatory if you are using a secure LDAP server connection. This field is only displayed when the Secure LDAP check box is selected.</td>
</tr>
</tbody>
</table>
| Windows Authentication | Specifies whether to use Windows Authentication or not. The options are:  
• None  
• Negotiate  
If you select the Negotiate option, the system displays the **Configuration for Windows Authentication** section. |

**Note:**  
Windows authentication is only supported if you are using a single authentication directory. If you are using multiple authentication directories, Windows Authentication is disabled.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Specifies the IP address or FQDN of the LDAP server.</td>
</tr>
<tr>
<td></td>
<td>If you are using the secure LDAP connection (LDAPS), you can only use the LDAP server FQDN. IP addresses are not supported.</td>
</tr>
<tr>
<td></td>
<td>This field is mandatory.</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the port of the LDAP server.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong></td>
</tr>
<tr>
<td></td>
<td>With the global catalog ports 3268 or 3269, LDAP queries can only return attributes marked for replication to the global catalog. For example, a user’s department cannot be returned because this attribute is not replicated to the global catalog. You must manually add all required attributes in the global catalog attributes list.</td>
</tr>
<tr>
<td></td>
<td>This field is mandatory.</td>
</tr>
<tr>
<td>Bind DN</td>
<td>Specifies the Distinguished Name (DN) of the user that has read and search permissions for the LDAP server users and roles. This is a mandatory setting.</td>
</tr>
<tr>
<td></td>
<td>The format of the Bind DN depends on the configuration of the LDAP server.</td>
</tr>
<tr>
<td></td>
<td>This field is mandatory.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>Even though the parameter name is Bind DN, the format of its value is not limited to the DN format. The format can be any format that the LDAP server can support for LDAP bind.</td>
</tr>
<tr>
<td></td>
<td>For example: for Active Directory, you can use &quot;domain\user&quot;, &quot;user@domain&quot;, as well as the actual DN of the user object.</td>
</tr>
<tr>
<td></td>
<td>For example: for Active Directory, you can use &quot;domain\user&quot;, &quot;user@domain&quot;, as well as the actual DN of the user object.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Bind Credential      | Specifies the password of the administrative user.  
The password length can be from 1 to 20 characters.  
The supported characters are:  
• Lowercase letters: a to z  
• Uppercase letters: A to Z  
• Numerics: 0 to 9  
• Special characters: exclamation point (!), at sign (@), percent (%), caret (^), asterisk (*), question mark (?), underscore (_), and dot (.). Special characters are not required for the password. |
| Base Context DN      | Specifies the complete Distinguished Name (DN) with the Organizational Unit (OU) for starting the search for users on the enterprise directory. This is the primary Base Context DN for Avaya Aura® Device Services. For example: dc=domain, dc=company, dc=com.  
If you are using multiple authorization domains, Avaya recommends including a domain component to the Base Context DN. For example: dc=avaya, dc=com.  

👍 Note:  
Some LDAP sources, such as Domino, typically do not contain the domain component in Base Context DNs. For example: o=MyCompany. If Base Context DNs do not contain the domain component, Avaya Aura® Device Services considers them “empty” Base Context DNs when processing user login or search requests. If Avaya Aura® Device Services cannot find the domain specified in the request, the search continues in “empty” Base Context DNs. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use additional Base Context DN</strong></td>
<td>Enables Avaya Aura® Device Services contact search and quick search. You can add up to 10 Base Context DNs with the same value. The primary Base Context DN is used for authentication. Additional Base Context DNs are used for Avaya Aura® Device Services contact search and quick search, and can also be used for authentication. If you select this check box, you can see the View/Edit button. Auto-configuration will use only the primary base context DN.</td>
</tr>
<tr>
<td><strong>View/Edit</strong></td>
<td>Enables access to the Addition Base DN Configuration page, where you can add or delete additional Base Context DNs.</td>
</tr>
<tr>
<td><strong>UID Attribute ID</strong></td>
<td>Specifies the unique attribute of the user on LDAP, which is used to search for users in the LDAP server.</td>
</tr>
<tr>
<td></td>
<td>If you are using multiple authentication domains, you must use one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• mail</td>
</tr>
<tr>
<td></td>
<td>• userPrincipalName</td>
</tr>
<tr>
<td></td>
<td>• Any custom attribute that uses a domain-qualified value.</td>
</tr>
<tr>
<td></td>
<td>If you are not using multiple authentication domains, you must use one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• uid, if you are using Open LDAP.</td>
</tr>
<tr>
<td></td>
<td>• sAMAccountName</td>
</tr>
<tr>
<td></td>
<td>• mail</td>
</tr>
<tr>
<td></td>
<td>• userPrincipalName</td>
</tr>
<tr>
<td></td>
<td>This field is mandatory.</td>
</tr>
<tr>
<td></td>
<td>Note:</td>
</tr>
<tr>
<td></td>
<td>When the UID attribute is set to “mail” on Open LDAP, use Apache Directory Studio to set the email value for the Open LDAP administrative user. This enables the administrative user to log in to the Avaya Aura® Device Services web administration portal using their email.</td>
</tr>
<tr>
<td><strong>Role Filter</strong></td>
<td>Specifies the search filter that is used to search the roles of the user.</td>
</tr>
<tr>
<td></td>
<td>For example: (&amp;(objectClass=group) (member={1}))</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Role Attribute ID</td>
<td>Specifies that the user is a member of the groups defined by that attribute. For example: objectCategory. This field is mandatory.</td>
</tr>
<tr>
<td>Roles Context DN</td>
<td>Specifies the complete Distinguished Name (DN) to search for a user role, that is, for Role Filter. For example: dc=domain,dc=company,dc=com.</td>
</tr>
<tr>
<td>Role Name Attribute</td>
<td>Specifies the name of the role attribute. This field is mandatory only if the Role Name Attribute Is DN field is set to true. For example: cn if the role is stored in a DN in the form of cn=admin, ou=Users, dc=company, dc=com.</td>
</tr>
<tr>
<td>Role Attribute is DN</td>
<td>Indicates whether the role attribute of the user contains DN. The default value is true.</td>
</tr>
<tr>
<td>Allow Empty Passwords</td>
<td>Indicates whether LDAP Server acknowledges the empty password. The default value is false.</td>
</tr>
<tr>
<td>Search Scope</td>
<td>Specifies the level of the search in the LDAP hierarchy. The options are: 0: For searching only for the object. 1: For including one level in the LDAP hierarchy in the search. 2: For including subtree in the LDAP hierarchy in the search. The default value is 2.</td>
</tr>
<tr>
<td>Role Recursion</td>
<td>Specifies whether role recursion is enabled. The options are: true false.</td>
</tr>
<tr>
<td>Administrator Role</td>
<td>Specifies the administrator role in which the administrative users are assigned.</td>
</tr>
<tr>
<td>Security Administrator Role</td>
<td>Specifies the security administrator role in which the administrative users can manage web certificates from the web administration portal.</td>
</tr>
<tr>
<td>User Role</td>
<td>Specifies the user role in which the common users are assigned.</td>
</tr>
</tbody>
</table>
### Auditor Role
Specifies the auditor role in which the users can audit the system.

### Services Maintenance and Support Role
Specifies the services maintenance and support role in which users can maintain and support services.

### Services Administrator Role
Specifies the services administrator role.

### Language used in Directory
- Simplified Chinese (zh)
- German (de)
- English (en)
- Spanish (es)
- French (fr)
- Italian (it)
- Japanese (ja)
- Korean (ko)
- Russian (ru)
- Portuguese (pt)

### Active Users Search Filter
Specifies whether the user is active or inactive on LDAP Server.

### Users Search Additional Filter
The search filter that provides extended search options in addition to **Active users search filter**. If you want to search for users using additional criteria other than whether a user is active, provide that criteria in this field.

For example, if you want to search for users in the object class “user” and the object category “Person”, use the following filter: `(&(objectClass=user)(objectCategory=Person))`.

### Last Updated Time Attribute ID
Specifies when the user is updated on LDAP. For example, `whenChanged`.
This field is mandatory.

### Configuration for Windows Authentication

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Principal Name (SPN)</td>
<td>Specifies the service principal name</td>
</tr>
<tr>
<td></td>
<td>UIDAttributeID must be userPrincipalName.</td>
</tr>
<tr>
<td>Import keytab file</td>
<td>Imports the <code>tomcat.keytab</code> file and overwrites the existing file.</td>
</tr>
</tbody>
</table>
### Configuring additional base context DNs

**About this task**

Use this procedure to add additional base context DNs. Additional base context DNs are used for Avaya Aura® Device Services contact search and quick search, and can also be used for authentication. You can add up to 10 base context DNs for one LDAP source.

If you are planning to use the additional base context DN for authorization, the role context DN configured in the primary LDAP will be used for this additional base context DN.

**Procedure**

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
   
   The system displays the Enterprise LDAP Server Configuration page.

2. Select the required LDAP server.

3. In the Server Address and Credentials section, select the **Use additional Base Context DN** check box and click **View/Edit**.

4. In the Additional Base Context DN Configuration window, click **+**.

5. Select the base context DN and in the **Base Context DN** field, provide the value of the base context DN.

6. If you want to use the base context DN for authentication, select the **Use for Authentication** check box.

7. Click **Save**.
Administering the LDAP server configuration

Procedure
1. On the Avaya Aura® Device Services web administration portal, navigate to Server Connections > LDAP Configuration > Enterprise Directory.
   The system displays the Enterprise LDAP Server Configuration page.
2. Select the required LDAP Server.
3. Modify the details of the enterprise directory.
4. Click Save.

Modifying enterprise directory attribute mappings

Procedure
1. On the Avaya Aura® Device Services web administration portal, navigate to Server Connections > LDAP Configuration > Enterprise Directory.
   The system displays the Enterprise LDAP Server Configuration page.
2. Select the required LDAP server.
3. In the Server Address and Credentials section, click Modify Attribute Mappings.
   The system displays the Enterprise Directory Mappings page.
4. In the Modify LDAP Attribute Mappings section, modify the value of the attributes.
5. Click Save.

Configuring Windows Authentication for Active Directory

About this task
Windows authentication is only supported if you are using a single authentication directory. If you are using multiple authentication directories, Windows Authentication is disabled.

Before you begin
Ensure that the LDAP server you use is the Domain Controller with the appropriate Active Directory version as the server type.

Procedure
1. On the Avaya Aura® Device Services web administration portal, navigate to Server Connections > LDAP Configuration > Enterprise Directory.
   The system displays the Enterprise LDAP Server Configuration page.
2. In the Server Address and Credentials section, do the following:
   a. In the **Windows Authentication** field, click **Negotiate**.
   b. In the Confirm Action pop-up window, click **OK**.
   c. The **UIDAttributeID** must be userPrincipalName.
   d. Ensure that the other settings on the Server Address and Credentials page are appropriate for the LDAP configuration of your Domain Controller.

3. In the Configuration for Windows Authentication section, do the following:

   **Tip:**
   To complete the following fields, use the same values you entered when setting up the Windows Domain Controller.

   a. In **Service Principal Name**, type **HTTP** or **REST_FQDN**.
      For example, type HTTP or aads.example.com.

   b. To import the **tomcat.keytab** file transferred from the Windows Domain Controller, in **Import keytab file**, click **Import**.
      In cluster deployments, the file is transferred to all nodes in the cluster. An additional option is available to send the file to specific nodes in a cluster.
      You can use the following command to generate a **tomcat.keytab** file.
      ```
      ktpass /out c:\tomcat.keytab /mapuser <Domain User Login>@<Kerberos realm> /princ HTTP/<FRONT-END_FQDN>@<Kerberos realm> /pass +rndPass /crypto all /kvno 0
      
      In the following example, <Domain User Login> is aads_spn_user, <Kerberos realm> is EXAMPLE.COM, and <FRONT-END_FQDN> is aads.example.com:
      ktpass /out c:\tomcat.keytab /mapuser aads_principal1@EXAMPLE.COM /princ HTTP/aads.example.com@EXAMPLE.COM /pass +rndPass /crypto all /kvno 0
      
      c. In **Kerberos Realm**, type the Kerberos realm, which is usually in uppercase letters.
         For example, EXAMPLE.COM.

   d. In **DNS Domain**, type the DNS domain of the Domain Controller.
      For example, example.com.

   e. In **KDC FQDN**, type the FQDN of the Domain Controller.
      This value also includes the DNS domain at the end.
      For example, ad.example.com.

   f. In **KDC Port**, do not change the default setting, which is 88.

   g. In a cluster deployment, click **Send Keytab File** to send the **tomcat.keytab** file to a specific node.
      This option is useful if the import to a node failed or if you add a new node to your cluster.
4. Save the settings to restart the server.

The settings you specified are used to generate the files needed to configure the Tomcat JAASRealm and the corresponding Sun JAAS Login module for GSS Bind.

---

### Modifying the provenance priority

**Procedure**

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.

   The system displays the Enterprise LDAP Server Configuration page.

2. Click the **Enterprise Directory** tab that you want to use to modify the provenance priority.

3. In the **Provenance Priority** field, click **Modify**.

   The system displays the Source Priority Configuration pop-up window.

4. In the **Provenance Priority** column, type the priority level.

   You can assign a value between 2 to 10. You cannot assign Provenance priority 1 as it is always assigned to the authorization directory. Provenance priority 1 is the highest and 10 is the lowest. Provenance priority must be different for each enterprise directory or source.

5. Click **Save**.

6. Restart Avaya Aura® Device Services to apply the new priority.

---

### Setting up user synchronization with the LDAP server

**Procedure**

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.

   The system displays the Enterprise LDAP Server Configuration page.

2. In the **User Synchronization Update Instructions** section, do the following:
   
   a. Specify a date and time to schedule the synchronization of Avaya Aura® Device Services users with the Enterprise LDAP server users.

   b. Select the **Repeat** check box and click the day to set up a recurring event for synchronization.

   c. Click **Save**.

3. **(Optional)** To immediately synchronize the user data, do the following:
   
   a. Click **Force LDAP Sync**.

   b. Click **Save**.
Configuring the internationalization parameters

About this task

The internationalization parameters specify how a user’s given name and surname are stored in Microsoft Active Directory (AD), as well as the language used to store these names. Optionally, for non-Latin script languages, two of the parameters also specify how the ASCII transliteration of these names is stored.

The following procedure describes how to configure the LDAP internationalization parameters when AD is used.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to Server Connections > LDAP Configuration > Enterprise Directory.

   The system displays the Enterprise LDAP Server Configuration page.

2. Configure the language setting:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language used in Directory</td>
<td>The language code of one of the languages supported by Avaya Aura® Device Services.</td>
<td>en</td>
</tr>
</tbody>
</table>

3. Click Save.

4. Click Modify Attribute Mappings.

5. Configure the following settings:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NativeFirstName</td>
<td>The attribute that stores the &quot;given name&quot; of the user in the language of the LDAP server.</td>
<td>givenName</td>
</tr>
<tr>
<td>NativeSurName</td>
<td>The attribute that stores the &quot;surname&quot; of the user in the language of the LDAP server.</td>
<td>sn</td>
</tr>
<tr>
<td>GivenName</td>
<td>This is only applicable if the language in AD is one of the non-Latin script based ones.</td>
<td></td>
</tr>
<tr>
<td>SurName</td>
<td>This is only applicable if the language in AD is one of the non-Latin script based ones.</td>
<td></td>
</tr>
</tbody>
</table>

The NativeFirstName and NativeSurName parameters allow the user to identify the LDAP attributes used to store the user's native language given name and surname. These are mandatory parameters with defaults of givenName and sn.

The GivenName and SurName parameters allows the user to identify the LDAP attributes used to store the ASCII transliteration of the user's given name and surname, respectively. These are optional parameters and only used only if the Language used in Directory parameter is set to one of the non-Latin script languages.
The internationalization of the names must be done using the language tags specified in [RFC 3866](https://tools.ietf.org/html/rfc3866).

To configure internationalization for Microsoft Active Directory, you must configure custom attributes for the native and the ASCII transliterations of the names, if both types of names are needed.

6. Click **Save** to apply changes and restart Avaya Aura® Device Services.

---

### Adding a trusted host

**Procedure**

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > Trusted Hosts**.
2. Click **Add**.
3. In the new row, type the FQDN or IP address of the trusted host.
   - When connecting to a cluster, add the IP address or FQDN of each node in the cluster and the virtual IP address of the cluster that you want Avaya Aura® Device Services to trust.
4. Click **Save**.

---

### Supported characters for LDAP attributes

For LDAP attributes, you can use the majority of special characters as is. The following are the exceptions:

- The userid attribute does not support the following characters:
  - Colon (:)  
  - Slash (/)  
  - Left brace ({)  
  - Right brace (})
- The basectxdn, rolesctxdn, and role attributes do not support the comma (,).

If you want to use quotation marks ("') or a backslash (\) in LDAP attributes, you must prepend these characters with a single backslash (\) character. For example, if you want to use the `backslash\` value for the `sAMAccountName` attribute, you need to enter it as `backslash\`.

---

### Updating user attributes in LDAP

**About this task**

In the enterprise directory, you cannot change the Distinguished Name (DN) of a user. Therefore, you cannot change other user attributes related to the DN, such as the Common Name (CN),
Organization Unit (OU), and Domain Component (DC). You also cannot update the user email address. To update user attributes in LDAP, you must de-register and then re-register the user after updating the required attributes.

Procedure

1. Log in to Avaya Aura® Device Services as an administrator.
2. Run the cduit misc command.
3. Run the following command to remove the user from the enterprise directory and from the database:
   
   ```
   sudo ./clitool-acs.sh runUserDiagnostics -d <email address of the user>
   ```
   
   For example:
   ```
   sudo ./clitool-acs.sh runUserDiagnostics -d email1@domain.com
   ```
   
   For more information about this command, see “runUserDiagnostics tool” in Deploying Avaya Aura® Device Services.
4. Update the attributes in the enterprise directory as required.
   For more information, see the documentation for the LDAP server you are using.
5. Log in to the Avaya Equinox® client to re-register the user on Avaya Aura® Device Services.

Open LDAP user data imports

You can upload user data to Open LDAP in bulk using the Avaya Aura® Device Services web administration portal. You can upload the following user data to Avaya Aura® Device Services:

- Given name
- Last name
- Email address
- Phone number
- User image
- Department

Users are uploaded using a ZIP archive, which contains the following:

- File in CSV format with user data.
- Directory containing user photos.

If you are planning to upload user photos, you must specify the path to these photos in the CSV file.

⚠️ Important:

The maximum image size is 50 KB.
For more information about the CSV file structure, see Structure of a CSV file for the bulk upload procedure on page 49.

⚠️ Important:
If you are planning to upload user photos to Open LDAP, you must set the PictureURL attribute to "jpegPhoto" first. For more information, see Changing the PictureURL attribute on page 51.

Structure of a CSV file for the bulk upload procedure

For uploading user data to Open LDAP, Avaya Aura® Device Services uses files in CSV format.

The first data record in a CSV file is a header. This header is not processed by Avaya Aura® Device Services and is used for informational purposes only. For example: Given Name, Last Name, Email Address, Phone Number, Image, Department

Each subsequent data record in a CSV file is a sequence of comma-separated user attributes in the following order:

<Given Name>,<Last Name>,<Email Address>,<Phone Number>,<Image>,<Department>

The following table describes these attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Is required</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Given Name</td>
<td>First name of the user</td>
<td>Yes</td>
<td>Aiden</td>
</tr>
<tr>
<td>Last Name</td>
<td>Last name of the user</td>
<td>Yes</td>
<td>Johnson</td>
</tr>
<tr>
<td>Email Address</td>
<td>Email address of the user</td>
<td>Yes</td>
<td><a href="mailto:aiden_johnson@company.com">aiden_johnson@company.com</a></td>
</tr>
<tr>
<td>Phone Number</td>
<td>Phone number of the user</td>
<td>Yes</td>
<td>123456789</td>
</tr>
<tr>
<td>Image</td>
<td>Relative path to the user photo in the image folder</td>
<td>No</td>
<td>Images/aiden_johnson.jpg</td>
</tr>
<tr>
<td>Department</td>
<td>Department of the user</td>
<td>No</td>
<td>Sales</td>
</tr>
</tbody>
</table>

For example:

Aiden, Johnson, aiden_johnson@company.com, 123456789, Images/aiden_johnson.jpg, Sales.

If you do not want to provide optional attributes, do not include these attribute values in the data record. For example, if you do not want to use user photos, provide the user attributes as follows: Aiden, Johnson, aiden_johnson@company.com, 123456789, , Sales.

The following is an example of a CSV file extract:

<table>
<thead>
<tr>
<th>Given Name, Last Name, Email Address, Phone Number, Image, Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aiden, Johnson, <a href="mailto:aiden_johnson@company.com">aiden_johnson@company.com</a>, 123456789, Images/aiden_johnson.jpg, Sales</td>
</tr>
<tr>
<td>James, Edwards, <a href="mailto:james_edwards@company.com">james_edwards@company.com</a>, 123450001, Support</td>
</tr>
<tr>
<td>Harry, Anderson, <a href="mailto:harry_anderson@company.com">harry_anderson@company.com</a>, 123451111, Images/harry_anderson.jpg, Support</td>
</tr>
</tbody>
</table>

To upload user photos, include a photo directory in a ZIP archive used for bulk import. The Photo attribute specifies the relative path to the user photo, starting from that directory.
For example, to upload a file called picture.jpg, which is located in a directory called Images, you must enter Images/picture.jpg.

If you are using Microsoft Excel to create the CSV file, you can provide each attribute in a separate column. If you do not want to provide certain attributes, leave the corresponding cells blank. For example:

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Given Name</td>
<td>Last Name</td>
<td>Email Address</td>
<td>Phone Number</td>
<td>Image</td>
</tr>
<tr>
<td>2</td>
<td>Aiden</td>
<td>Johnson</td>
<td><a href="mailto:aiden_johnson@company.com">aiden_johnson@company.com</a></td>
<td>123456789</td>
<td>Images/aiden_johnson.jpg</td>
</tr>
<tr>
<td>3</td>
<td>James</td>
<td>Edwards</td>
<td><a href="mailto:james_edward@company.com">james_edward@company.com</a></td>
<td>123450001</td>
<td></td>
</tr>
</tbody>
</table>

**Uploading users in bulk**

**About this task**

Use this procedure to upload user data to Open LDAP.

- If you want to upload user photos, you must upload a ZIP archive, which contains a CSV file with user data and a directory with user photos.
- If you do not need to upload user photos, you can upload a CSV file with user data. Packaging the CSV file in a ZIP archive is not required.

In a cluster environment, you only need to upload user data to a single node. The user data will be replicated to all other nodes in the cluster.

If a user you are uploading already exists, the user data will be overwritten.

You can only perform this procedure if Open LDAP is installed on Avaya Aura® Device Services.

**Before you begin**

- Create a CSV file with the user data you want to upload on Avaya Aura® Device Services.
- Ensure that the PictureURL LDAP attribute is set to “jpegPhoto”. For more information, see Changing the PictureURL attribute on page 51.

**Procedure**

1. If you want to upload user photos, package the CSV file and the directory containing user photos into a ZIP archive with no intermediate directories.
2. On the Avaya Aura® Device Services web administration portal, navigate to Server Connections > Bulk Import Users.
3. Click Choose File and select either the ZIP archive or the CSV file with user data.
4. In Default Password for All Users, provide a password to be used for all users you are importing.
5. Click Upload.
Changing the PictureURL attribute

About this task
Use this procedure if you are using onboard Open LDAP and want to upload user images.

Procedure
1. Log in to the Avaya Aura® Device Services web administration interface.
2. Navigate to Server Connections > LDAP Configuration.
3. On the Enterprise Directory page, select the onboard Open LDAP tab.
4. Click Modify Attributes Mapping.
5. For PictureURL, select jpegPhoto from the drop-down list.
6. Click Save.
7. To apply the changes immediately, click Force LDAP Sync on the Enterprise Directory page.

Cross-origin resource sharing

Using the Cross-origin resource sharing (CORS) technology, you can access the webpage resources from different domains. With CORS, a browser can send a cross-origin HTTP request to the web servers to access the resources from a different domain. Also it facilitates a secure cross-domain data transfer.

You can enable and configure CORS on the Avaya Aura® Device Services server using the Avaya Aura® Device Services web administration portal or the Avaya Aura® Device Services configuration utility.

You can enable CORS for the service and administrator interfaces.

Service Interface
The Service Interface page displays the CORS configuration for the Avaya Aura® Device Services server using service port 443.

Administrator Interface
The Admin Interface page displays the CORS configuration for the Avaya Aura® Device Services server using port 8445.

Enabling Cross-origin resource sharing for the Service Interface

Procedure
1. On the Avaya Aura® Device Services web administration portal, navigate to Server Connections > CORS Configuration > Service Interface.
The system displays the Cross-Origin Resource Sharing for Service interface page.

2. Select the **Enable Cross-Origin Resource Sharing** check box.
   
The system displays the **Allow access from any origin** and **Specific Domain(s)** fields.

3. Do one of the following:
   
   • To allow access to the Avaya Aura® Device Services resources from any domain, select the **Allow access from any origin** check box.
   
   • To allow access to the Avaya Aura® Device Services resources from specific domains, in the **Specific Domain(s)** field, type the comma-delimited list of the domain names.

4. Click **Save**.

   The system saves the specified CORS configuration in the Cassandra database and in `/opt/Avaya/DeviceServices/<aads_version>/nginx/1.8.0-1/conf/cors-service.conf`. The system then reloads the Avaya Aura® Device Services Nginx configuration to apply CORS changes.

   For service interface, the system applies the CORS configuration for the root `/`.

---

**Enabling Cross-origin resource sharing for the Administrator Interface**

**Procedure**

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > CORS Configuration > Admin Interface**.
   
The system displays the Cross-Origin Resource Sharing for Admin interface page.

2. Select the **Enable Cross-Origin Resource Sharing** check box.
   
The system displays the **Allow access from any origin** and **Specific Domain(s)** fields.

3. Do one of the following:
   
   • To allow access to the Avaya Aura® Device Services resources from any domain, select the **Allow access from any origin** check box.
   
   • To allow access to the Avaya Aura® Device Services resources from specific domains, in the **Specific Domain(s)** field, type the comma-delimited list of the domain names.

4. Click **Save**.

   The system saves the specified CORS configuration in the Cassandra database and in `/opt/Avaya/DeviceServices/<aads_version>/nginx/1.8.0-1/conf/cors-service.conf`. The system then reloads the Avaya Aura® Device Services Nginx configuration to apply CORS changes.

   The system applies the specified CORS configuration for the administrator interface to `/admin/webdeployment/upload URL`, for example, `https://<aads_server>:8445/admin/webdeployment/upload`. 
Web Deployment service management

The Web Deployment service enables appcast for Avaya Equinox® desktop clients. On the Web Deployment page, you can add, edit, or delete an appcast item from the appcast table at the bottom of the page.

The Web Deployment service supports the upload and download of the client installer, which includes software update files. The system creates the upload folder automatically during a deployment or upgrade. You can also store files to be downloaded later. The files can be downloaded from https://<aads_server_address>:443/acs/resources/webdeployment/downloads/<file_name_with_extension>. The upload service operates from the directory https://<aads_server_address>:8445/admin/webdeployment/upload/.

Settings for receiving the updates from a client installer

The Dynamic Configuration service has the following three settings for the Web Deployment service:

- APPCAST_ENABLED
- APPCAST_CHECK_INTERVAL
- APPCAST_URL

If the value of the APPCAST_ENABLED settings is set to true, the Avaya Equinox® client will get the APPCAST_URL setting from the Dynamic Configuration service response for the Web Deployment service.

The APPCAST_URL must be set to https://<IP address of the AADS Server>:443/acs/resources/webdeployment.

Web Deployment port configuration

By default, the Web Deployment service uses port 443. Optionally, you can configure Avaya Aura® Device Services to use port 8442 for the Web Deployment service. For more information, see Running a patch to allow Avaya Equinox for Windows to connect to the Web Deployment service on page 129.

Note:

For upload URLs that point to the Web Administration interface, port 8445 is used. These URLs contain /admin after the address and port values. For example: https://aads.server.com:8445/admin/webdeployment/upload

Uploading the client installer

About this task

Use this procedure to upload and download the client installer for the Web deployment service.
For Avaya Equinox® for Windows, you can upload .exe or .msi installation files. For Avaya Equinox® for Mac, you can upload .dmg installation files, which are packaged in a .zip archive.

**Procedure**

1. Download Avaya Equinox® for Mac or Avaya Equinox® for Windows installation files from the Avaya Support website.

   **Note:**
   You must have PLDS access to download these files.

2. If you are uploading Avaya Equinox® for Mac, pack the Avaya Equinox-<version>.dmg and Avaya Equinox Sparkle Update-<version>.dmg files into a .zip archive with no intermediate directories.

   If the .zip archive contains intermediate directories, re-pack the archive so that it only contains the .dmg files in the root directory.

3. Log on to the Avaya Aura® Device Services web administration portal.

4. On the Avaya Aura® Device Services web administration portal, navigate to **Web Deployment** > **Deployment**.

   The system displays the Software Update Deployment page.

5. In the **Title** field, type the name of the updates or appcast for the client installer.

   When you type the name of the updates for the client installer, the system automatically adds Avaya Equinox before the given title.

   For example, if you type the update name: *Windows Version 2.0: Critical update*

   The system displays: *Avaya Equinox for Windows Version 2.0: Critical update*

6. In the **Description** field, type the description of the client installer updates.

   For more information, see the Release Notes for the new client installer.

7. In the **Version** field, type the version detail for the Avaya Equinox® client release.

8. In the **OS** field, select one of the following platforms for the Avaya Equinox® client release:
   - Windows
   - Macintosh

9. Do one of the following:
   - If you are uploading an Avaya Equinox® for Mac client installer which requires a specific macOS version, in the **Min OS version** field, provide the minimum macOS version that is supported by the client.

     For example: *9.3.0* or *10.4.5.0*.

   - If you are uploading an Avaya Equinox® for Mac client installer which does not require a specific macOS version, leave the **Min OS version** field blank.
• If you are uploading an Avaya Equinox® for Windows client installer, leave the Min OS version field blank.

10. In File, click Choose File and select one of the following files to upload:
• For Avaya Equinox® for Windows, select the .exe or .msi installation file.
• For Avaya Equinox® for Mac, select the .zip archive containing the .dmg installation files.

The maximum upload size for the client installer is 100 MB. The upload service accepts alphanumeric characters, white spaces, dots, minus, and square brackets.

After you upload the file, the system auto populates the Size (in bytes) and the MD5 Hash field.

11. In the Upload URL(s) field, choose one of the following, and then click Upload:
• Default: To upload the client installer to the Avaya Aura® Device Services server. This is the default option. You cannot edit the value of the default URL.
• Custom: To provide a URL of a different server for uploading the client installer.

The system displays a pop up to specify the user credentials to upload the client installer and a confirmation dialog box to indicate the upload status.

12. In the Download URL(s) field, choose one of the following:
• Default: To download the client installer from the Avaya Aura® Device Services server to the clients. This is the default option. You cannot edit the value of the default URL.
• Custom: To provide a URL of a different server for downloading the client installer.

To download the client installer, you must enter the credentials for client authentication.

13. Click Save to save the settings.

The system populates the data in the table at the bottom of the page. For more information about fields, see Appcast items field descriptions on page 55. To edit or delete a specified setting, you can double-click to select an entry.

Appcast items field descriptions

The Appcast Items table shows the list of Avaya Equinox® client installers which you can download using the Web Deployment service.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The name of the updates or appcast for the client installer.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the client installer updates or appcast.</td>
</tr>
<tr>
<td>Version</td>
<td>The version information for the Avaya Equinox® client release.</td>
</tr>
<tr>
<td>Publish Date</td>
<td>The date and time when the installer was uploaded onto the Web Deployment service.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OS</td>
<td>The platform of the Avaya Equinox® client installer.</td>
</tr>
<tr>
<td>Download URL</td>
<td>The URL that specifies the location of the Avaya Equinox® client installer.</td>
</tr>
<tr>
<td>Downloads</td>
<td>The number of times the appcast file has been downloaded using the download URL.</td>
</tr>
</tbody>
</table>
| Updates      | The number of times the upgrade file was applied on the already installed client using the respective appcast file download URL. This counter increases if a user does the following:  
  • Tries to download the client from Unified Portal, and Unified Portal detects that the user already has an installed version of the client.  
  • Updates the client using the built-in Check for Updates option. |

### Editing an appcast item

**Procedure**

1. On the Avaya Aura® Device Services web administration portal, navigate to **Web Deployment > Deployment**.  
   The system displays the Software Update Deployment page.
2. On the bottom of the Software Update Deployment page, double-click an entry in the table.  
   The system displays the Edit appcast item page.
3. Edit the settings that you want to change.
4. Click **Save**.  
   The system populates the updated data in the table at the bottom of the page.

### Deleting an appcast item

**Procedure**

1. On the Avaya Aura® Device Services web administration portal, navigate to **Web Deployment > Deployment**.  
   The system displays the Software Update Deployment page.
2. On the bottom of the Software Update Deployment page, click an entry in the table.  
   The system displays the Edit appcast item page.
3. Click **Delete**.
The system displays the Delete item page.

4. Click **Yes**.

---

**Reviewing download statistics**

**About this task**

The Download statistics table shows the total number of Avaya Equinox® clients installations and updates performed using the Web Deployment service. The statistic table includes data for both installers currently available for downloading and installers which have been removed from Web Deployment.

**Procedure**

1. On the Avaya Aura® Device Services web administration portal, navigate to **Web Deployment > Deployment**.
2. Navigate to the Download statistic table at the bottom of the page.

   For more information about options in the table, see [Download statistics field descriptions](#) on page 57.

**Download statistics field descriptions**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>The platform of the Avaya Equinox® client installer.</td>
</tr>
<tr>
<td>Fresh Install</td>
<td>The total number of fresh installation attempts for the Avaya Equinox® clients for the given OS using the Web Deployment service.</td>
</tr>
<tr>
<td>Updates</td>
<td>The total number of attempts to update the Avaya Equinox® clients for the given OS using the Web Deployment service.</td>
</tr>
<tr>
<td>Total</td>
<td>The total number of fresh installation and update attempts for the Avaya Equinox® clients for the given OS using the Web Deployment service.</td>
</tr>
</tbody>
</table>

---

**Managing picture settings**

**About this task**

Use this procedure to manage whether users can upload their own photos.

**Procedure**

1. On the Avaya Aura® Device Services web administration portal, navigate to **Pictures > Configuration**.
The system displays the Pictures Configuration page.

2. Select the **Allow users to upload their own photos** check box.

3. Click **Save**.
Chapter 4: Working with the Utility Server

Utility Server overview

You can enable the Utility Server when you install or upgrade Avaya Aura® Device Services. The Utility Server offers the following:

- File server functionality. The Utility Server hosts various files that Avaya phones require to operate, such as firmware, configuration, or upgrade files.
- Firmware management. The Utility Server provides the option to upload new phone firmware to the file server. You can also activate or deactivate the firmware.

⚠️ Important:

- You cannot enable the Utility Server using the Avaya Aura® Device Services web administration portal or configuration utility.
- Although 46xxsettings.txt files are generated using the Dynamic Configuration service, these files are stored on the Utility Server. Therefore, you cannot generate 46xxsettings.txt files if you do not enable the Utility Server.

Utility Server in a cluster environment

The Utility Server is not clustered. When you upload files, such as firmware packages or upgrade files, on a Utility Server node, these files are not available on other cluster nodes. You must upload these files on all other Utility Server instances manually.

⚠️ Note:

Configuration files generated using the Dynamic Configuration service become available on all cluster nodes automatically.

Browser support

You can access the Utility Server functionality using the following browsers:

- Google Chrome
- Internet Explorer

Mozilla Firefox does not support certain features, such as backup and restore.
Utility Server capacity limits

Depending on the Avaya Aura® Device Services deployment method, the Utility Server has the following capacity limits for firmware files:

- If Avaya Aura® Device Services is installed on an AVP host, then the total size of firmware .zip files or unpacked firmware packages uploaded on the Utility Server must not exceed 6 GiB.

- If Avaya Aura® Device Services is installed on an ESXi host or AWS AMI instance, then the total size of firmware .zip files or unpacked firmware packages uploaded on the Utility Server must not exceed 12 GiB.

Setting up a DHCP server

About this task

Configure a DHCP server to allow IP phones to locate the Utility Server in the network. Avaya Aura® Device Services supports any DHCP server software as long as the software is correctly configured.

Before you begin

Contact your DHCP server software vendor to obtain server software installation and configuration instructions.

Procedure

1. Install the DHCP server software according to the server software vendor's instructions.

2. On your DHCP server, configure option 242 as follows:

   "TLSSRVR=<Utility Server IP address or FQDN>,TLSPORT=1543,TLSSRVRID=0,HTTPSRVR=<Utility Server IP address or FQDN>,HTTPPORT=80,MCIPADD=<H.323 call server address list>"

   For example:

   "TLSSRVR=1.2.3.4,TLSPORT=1543,TLSSRVRID=0,HTTPSRVR=1.2.3.4,HTTPPORT=80,MCIPADD=3.5.7.9"

   • Only H.323 endpoints use MCIPADD.
   • Firmware and custom files for SIP endpoints use HTTPS, so HTTPSRVR and HTTPPORT are not required if you are only using SIP endpoints.

3. Configure other DHCP settings, such as the available range of IP addresses, as required.

   For information about other DHCP options you can configure, see http://downloads.avaya.com/elmodocs2/one-X_Deskphone_Edition/R1.5/output/16_300698_4/admin055.html#527056.
Starting and stopping the Utility Server

Procedure

1. Log in to the Avaya Aura® Device Services as an administrator using an SSH connection.
2. Run one of the following commands:
   • `svc utilserv start` to start the Utility Server.
   • `svc utilserv stop` to stop the Utility Server.
   • `svc utilserv restart` to restart the Utility Server.

Logging in to the Utility Server

Procedure

1. Open the Google Chrome or Internet Explorer browser.
   Replace `Utility_Server_address` with the virtual IP address or FQDN of the Utility Server.
3. On the Login screen, enter the user name and password of the administrative user that you created during the OVA deployment.

Related links

- Monitoring cluster nodes on page 97

Reviewing the disk space occupied by firmware package files

About this task

Use this procedure to ensure that the Utility Server has enough free space to store a firmware package that you want to upload or unpack.

Procedure

- To check the amount of space occupied by uploaded firmware `.zip` files, run the following command:
  ```bash
  sudo du -hs /tmp/*.*.zip
  ```

  The output value must not exceed the following values:
  - 6 GiB if Avaya Aura® Device Services is installed on an AVP host.
- 12 GiB if Avaya Aura® Device Services is installed on an AWS AMI or an ESXi host.

If the output value exceeds the listed sizes, you must remove some .zip files from the Utility Server before uploading new firmware packages.

• To check the amount of space occupied by unpacked firmware packages, run the following command:

```
sudo du -hs /opt/IPPhoneFirmware
```

The output value must not exceed the following values:

- 6 GiB if Avaya Aura® Device Services is installed on an AVP host.
- 12 GiB if Avaya Aura® Device Services is installed on an AWS AMI or an ESXi host.

If the output value exceeds the listed values, you must remove some unpacked firmware packages before unpacking another package.

---

### Uploading files on the Utility Server

#### About this task

Use this procedure to upload files, such as firmware packages, on the Utility Server. You can upload a single file or an archive in the .zip format. The Utility Server stores the uploaded files in the /tmp directory.

---

#### Important:

In a cluster environment, you must manually upload a firmware package on each Utility Server node. Avaya Aura® Device Services does not automatically copy files uploaded to one node onto other cluster nodes.

#### Before you begin

• Configure a DHCP server. For more information, see Setting up a DHCP server on page 60.
• Ensure that you have enough free disk space to upload a firmware package. For information about reviewing disk space, see Reviewing the disk space occupied by firmware package files on page 61.

#### Procedure

1. On the Utility Server web interface, in the navigation pane, click **Upload Files**.
2. On the Upload File screen, click **Browse**.
3. Select the required file and click **Open**.
   
   The Utility Server displays the selected file name to the right of the **Browse** button.
4. Click **Upload File**.

   The uploading process can take some time depending on the file size and connection speed.
If you upload a firmware package, it appears in the “Firmware package” table on the Manage Phone Firmware tab.

---

### Uploading an IP phone custom file

**About this task**

Use this procedure to upload custom files or site-specific files, such as custom screen saver images, wallpaper images, or ringtones, to the Utility Server. You can upload a single file or a .zip archive. The files are available immediately after uploading. The Utility Server overwrites existing files.

The Utility Server stores uploaded custom files in the `/var/www/html/custom` directory.

**Before you begin**

Configure a DHCP server. For more information, see [Setting up a DHCP server](#) on page 60.

**Procedure**

1. On the Utility Server web interface, in the navigation pane, click **IP Phone Custom File Upload**.
2. On the IP Phone Custom File Upload screen, click **Browse**.
3. Select the required file and click **Open**.
   
   The Utility Server displays the file name to the right of the **Browse** button.
4. Click **Upload Custom Files and Activate**.

---

### Viewing custom files uploaded on the Utility Server

**Procedure**

1. On the Utility Server web interface, in the navigation pane, click **IP Phone Custom File Upload**.
2. Click **Display Custom Directory**.

   The Utility Server displays a table containing the following information about the uploaded custom files:
   
   - The name of the custom file.
   - The file size.
   - The last modification date.
Accessing IP phone custom files

About this task

IP phones can directly access the custom files that you upload on the Utility Server.

Procedure

Depending on the protocol you are using to access files, use one of the following URLs:

- To access custom files using the HTTP protocol, use the `<IP or FQDN>:80/custom/<file_name>` URL. In the URL, `<IP or FQDN>` can be one of the following:
  - Avaya Aura® Device Services server IP address
  - Utility Server virtual IP address
  - Avaya Aura® Device Services server FQDN
  - Utility Server virtual FQDN

- To access custom files using the HTTPS protocol, use the `<virtual IP or FQDN>:1543/custom/<file_name>` URL. In the URL, `<virtual IP or FQDN>` can be one of the following:
  - Utility Server virtual IP address
  - Utility Server virtual FQDN

Backing up H.323 phone settings on the Utility Server

About this task

Use this procedure to back up H.323 phone settings, such as contact list, ring volume, and ring tone settings, on the Utility Server.

⚠️ Important:

The Utility Server does not support the backup of SIP phone settings.

The Utility Server stores phone settings in a text file. The name of this file contains the MAC ID or serial number of the phone. In a cluster environment, phone settings are stored on the seed node.

When you back up the Utility Server, the backup includes phone settings.

Before you begin

Configure a DHCP server. For more information, see Setting up a DHCP server on page 60.

Procedure

1. Run the following commands to enable port 80 on the server:

   ```
cdto misc
sudo ./us-http-port.sh --enable
   ```
For more information about this command, run the `sudo ./us-http-port.sh --h` command.

2. Log in to your phone and perform a manual backup.

   For more information about performing a manual backup on your phone, see the documentation for your phone model.

   The backup file is created on the server in the `/PhoneBackup` directory. For example: `/PhoneBackup/17774441530_96xxdata.txt`.

3. Reboot the phone.

4. Add the following entry to the `46xxsettings.txt` file for the phone model:

   ```
   SET BRURI http://<username>:<password>@<AADS IP address>/PhoneBackup
   ```

   `<username>` and `<password>` are credentials of the administrative user that you created during the OVA deployment.

   In a cluster environment, `<AADS IP address>` is the virtual IP of the cluster.

   For example: `SET BRURI http://administrator:password@1.2.3.4/PhoneBackup`.

---

### Utility Server backup and restore

#### Backing up data stored on the Utility Server

**About this task**

Use this procedure to back up data stored on the Utility Server, such as upgrade scripts or `46xxsettings.txt` files. The Utility Server backs up files that are stored on the Utility Server's web browser.

In a cluster environment, perform the backup procedure from the seed node.

**Note:**

- The Utility Server does *not* back up firmware files. After backing up and restoring the Utility Server, you need to manually re-upload and activate the required firmware packages.
- Backing up Avaya Aura® Device Services does *not* back up the Utility Server data.

**Procedure**

1. On the Utility Server web interface, in the navigation pane, click **Utility Services Backup and Restore**.
2. Click **Create Backup**.

   If the backup is completed successfully, the Utility Server displays the path to the backup file and the link to download the file.

3. Click **Download the newly created Utility Services Backup File** and save the backup file on an external storage device.

4. Click **Continue**.

---

**Restoring the Utility Server data**

**About this task**

Use this procedure to restore the Utility Server data from the backup file. The following rules apply when restoring the Utility Server data:

- All binaries that were activated before the backup procedure will be activated during the restore procedure.
- 46xxsettings.txt files, which were generated using the Dynamic Configuration service and stored in folders with groupIDs, will be restored in the same folders.

**Procedure**

1. Log in to the Utility Server.
2. On the Utility Server web interface, in the navigation pane, click **Utility Services Backup and Restore**.
3. From the **Upload and Restore Utility Server Backup File** field, select **Browse** and navigate to the backup file.
4. Click **Upload Backup**.

   When the restore procedure is complete, the Utility Server displays the procedure status.
5. In a cluster environment, repeat the steps above for all other nodes in the cluster.

---

**Backup and restore of phone model to group ID mapping**

When you back up the Utility Server data, phone model to group ID mapping is not backed up. Phone model to group ID mapping is maintained in the database. Therefore, to back up and restore this mapping, you must back up the Cassandra database as part of the Avaya Aura® Device Services backup procedure.

If the Avaya Aura® Device Services backup does not include the database backup, but the Utility Server was backed up and restored, then the restored system will not have phone model to group ID mapping. 46xxsettings.txt files will still be stored in group ID folders, but these folders will not be mapped to the correct phone models. In this case, you must manually assign group IDs to the phone models as described in [Assigning a group identifier to a phone model](#) on page 75. Otherwise, phones cannot download 46xxsettings.txt files from the Utility Server.
Firmware management

The following sections describe the firmware management operations available on the Utility Server.

Viewing firmware packages available on the Utility Server

Procedure

1. On the Utility Server web interface, in the navigation pane, click **Manage phone Firmware**.

   Firmware packages available on the system are listed in the “Firmware Package” table. The table also contains package status information:
   
   • Packed: Package is uploaded on the Utility Server.
   • Unpacked: Package content is extracted and ready to be activated.
   • Active: Phones can download the package content.

   For more information about package statuses, see Firmware package statuses on page 67.

2. To review the firmware package information, select the required package and click **View**.

Firmware package statuses

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packed</td>
<td>The firmware package is uploaded on the Utility Server.</td>
</tr>
<tr>
<td></td>
<td>When the firmware package has this status, you can perform the following actions:</td>
</tr>
<tr>
<td></td>
<td>• View information about the package.</td>
</tr>
<tr>
<td></td>
<td>• Unpack the package.</td>
</tr>
<tr>
<td></td>
<td>• Remove the .zip archive with the package from the Utility Server.</td>
</tr>
</tbody>
</table>
### Unpacking a firmware package

#### About this task

Before making the uploaded firmware available for phones to download, you must unpack the firmware package content. The Utility Server stores uploaded firmware packages in the `/tmp` directory. When you unpack the package, the Utility Server places the firmware files into the `/opt/IPPhoneFirmware/<package_name>` directory. For example, if you unpack the `96x1-IPT-H323-R6_6_4_01-102616.zip` package, the Utility Server places its content into the `/opt/IPPhoneFirmware/96x1-IPT-H323-R6_6_4_01-102616` directory.

During the unpacking procedure, the Utility Server checks the signatures of firmware files. If the signatures are not valid, then the files will not be unpacked and the Utility Server will display an error message.

#### Status Description

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unpacked</td>
<td>The firmware package files are extracted but cannot be downloaded by the phones. The Utility Server places the unpacked files in the <code>/opt/IPPhoneFirmware/&lt;package_name&gt;</code> directory. For example, if the package name is <code>96x1-IPT-H323-R6_6_4_01-102616</code>, it will be placed in the <code>/opt/IPPhoneFirmware/96x1-IPT-H323-R6_6_4_01-102616</code> directory. When the firmware package has this status, you can perform the following actions: • View information about the package. • Activate the package. • Remove the extracted files from the <code>/opt/IPPhoneFirmware/&lt;package_name&gt;</code> directory. The <code>.zip</code> archive with the firmware package will still be available on the Utility Server.</td>
</tr>
<tr>
<td>Active</td>
<td>Phones can download content from a package with this status. When the package is active, the Utility Server creates symbolic links to all package files and also copies the upgrade script from the package into the <code>/var/www/html</code> directory. When the firmware package has this status, you can perform the following actions: • View information about the package. • Deactivate the package. The package content is no longer available for phones to download, but the extracted files are still stored on the Utility Server. Note: You cannot remove firmware package files from the Utility Server if the package is active.</td>
</tr>
</tbody>
</table>

---

Comments on this document? infodev@avaya.com
error message. You can skip the signature check by selecting the **Forcibly Unpack** option, but it is not recommended.

**Before you begin**
Upload the firmware package onto the Utility Server.

**Procedure**
1. On the Utility Server web interface, in the navigation pane, click **Manage Phone Firmware**.
2. From the **Firmware Package** table, select the required package with the “Packed” status.
3. Unpack the firmware package using one of the following options:
   - **SHA256 Unpack**: Extracts files from a SHA256 signed firmware package.
   - **SHA1 Unpack**: Extracts files from a SHA1 signed firmware package.
   - **Forcibly Unpack**: Extracts files from a firmware package without signature checking.

**Note:**
- Avaya recommends that you use an SHA256 signed firmware package and always check the signatures of firmware files.
- You cannot unpack a SHA256 signed firmware package using the **SHA1 Unpack** option or SHA1 signed firmware package using the **SHA256 Unpack** option.

After the unpacking procedure is completed, the Utility Server displays the procedure status.
4. Click **Continue**.
   The firmware now has the “Unpacked” status in the “Firmware Package” table.

---

**Activating a firmware package**

**About this task**
Use this procedure to make an unpacked firmware package available for phones to download. During this procedure, the Utility Server creates symbolic links for all files in the `/opt/IPPhoneFirmware/<package_name>` directory and also copies the upgrade file from the package directory into the web server root directory, `/var/www/html`.

**Before you begin**
Unpack the required firmware package.

**Procedure**
1. On the Utility Server web interface, in the navigation pane, click **Manage Phone Firmware**.
2. Select the required firmware package that has the “Unpacked” status.
3. Click **Activate**.
4. Click **Continue**.

The firmware package version has the “Active” status in the “Firmware package” table.

**Next steps**

Update the path to the 46xxsettings.txt file in the upgrade file.

**Related links**

[Updating the path to the 46xxsettings.txt file in an upgrade file](#) on page 70

---

### Updating the path to the 46xxsettings.txt file in an upgrade file

**About this task**

Phones start the upgrade procedure by downloading and interpreting the content of the upgrade file. This file contains upgrade instructions, including information about downloading the 46xxsettings.txt file. You must update the default path to the 46xxsettings.txt file, which is specified in the upgrade file. This enables the phone to download the 46xxsettings.txt file generated by Avaya Aura® Device Services and stored on the Utility Server.

**Note:**

The file name of the upgrade model is based on the phone model. For example, 96x1 phones use the 96x1Hupgrade.txt file name.

**Before you begin**

- Activate the firmware package for the phone model.
- Assign the group identifier to the phone model on the Avaya Aura® Device Services web administration portal.

**Procedure**

1. Log in to the Avaya Aura® Device Services as an administrator using an SSH connection.
2. Run the `cd /var/www/html` command to navigate to the directory where the Utility Server stores upgrade files for activated firmware packages.
3. Open the required upgrade file in a text editor, such as vi.

   For example, to open the upgrade file for 96x1 series phones in vi, use the `vi 96x1Hupgrade.txt` command.

4. In the upgrade file, replace the `GET 46xxsettings.txt` entry with `GET <GroupID>/46xxsettings.txt`, where `<GroupID>` is the group identifier assigned to the phone model.

   For example, if you assigned 123 to the 96x1 phone model, the updated entry must look as follows: `GET 123/46xxsettings.txt`.
5. Save the upgrade file.
Deactivating a firmware package

About this task
Use this procedure if you no longer need a certain firmware package to be available for phones to download. For example, you can use this procedure when a new firmware version is available.

Procedure
1. On the Utility Server web interface, in the navigation pane, click Manage Phone Firmware.
2. From the “Firmware package” table, select the required version with the “Active” status.
3. Click Deactivate.
4. Click Continue.
   The firmware package version has the “Unpacked” status.

Removing a firmware package

About this task
Use this procedure if you want to remove a certain firmware package from the system. You cannot remove a firmware package with the “Active” status.

Procedure
1. On the Utility Server web interface, in the navigation pane, click Manage Phone Firmware.
2. From the Firmware Package table, select the firmware package you want to remove.
3. Click Remove.
   Depending on the current status of the firmware package, removing the package results in one of the following:
   • If the firmware package status is “Unpacked”, the firmware package status becomes “Packed”. The Utility Server removes all package files from the /opt/IPPhoneFirmware/<package_name> directory. The archive file still exists in the /tmp directory and is available for unpacking.
   • If the firmware package status is “Packed”, the Utility Server removes the package from the system. If you want to use this package again, you must re-upload this file onto the Utility Server.
Chapter 5: Administration of the Dynamic Configuration service

With the Dynamic Configuration service, the system can dynamically retrieve and deploy device configuration settings to the Avaya Equinox® clients. You can also use the Dynamic Configuration service to manage configuration settings and generate 46xxsettings.txt files for the following endpoints:

- Avaya Vantage™.
- Avaya J100 Series IP Phones.
- 9600 Series IP Deskphones.

Avaya Aura® Device Services generates a separate 46xxsettings.txt file for each endpoint category. Generated 46xxsettings.txt files are stored on the Utility Server.

Dynamic configuration provides a centralized place to administer user, group, platform, global, and exception settings. You can configure the device configuration settings on the Avaya Equinox® clients using one of the following methods:

- DNS-based auto discovery.
- Web address: On the Avaya Equinox® clients, type the Auto Configuration or Device Configuration URL.
  
  For example: https://<IP address>:443/acs/resources/configurations.

For information about how to configure DNS-based auto discovery and other settings on the Avaya Equinox® clients, see Planning for and Administering Avaya Equinox® for Android, iOS, Mac, and Windows.

**Note:**

The authentication domain is an enterprise directory with the Use for authentication check box selected. If a user belongs to an authentication domain and a group that is not in the authentication domain, the Dynamic Configuration service still works correctly.

Using the Dynamic Configuration service, you can configure and publish the configuration settings for the following:

- **Global:** The global settings can be overridden by any other settings category. The Global settings are used for both Avaya Equinox® clients and deskphones.

---

1 The endpoints are Avaya Vantage™ and supported hard phones, including the J100 and 9600 series phones. For Avaya Equinox®, the term “client” is used in the scope of this document.
• **Group:** The group specific settings can be overridden by user, platform, exception, and System Manager settings. The LDAP groups are ordered alphabetically. The Group settings are only used for Avaya Equinox® clients.

If a user belongs to more than one group on the LDAP server, Avaya Aura® Device Services applies settings according to the alphabetical order of the groups.

**Note:**

When a user or client requests automatic configuration, Avaya Aura® Device Services searches for user groups only in the configured contexts on the LDAP server containing the user.

For example, Avaya Aura® Device Services uses two LDAP servers configured as follows:

- LDAP 1 has the primary base context DN set to PrimaryBase1 and two additional base contexts, Base 2 and Base 3.
- LDAP 2 has the primary base context DN set to PrimaryBase2 and two additional base contexts, Base 4 and Base 5.

In this case, for a user that is in LDAP 1, Avaya Aura® Device Services only searches for groups in PrimaryBase1, Base 2, and Base 3.

• **User:** The user specific settings can be overridden by platform, exception, and System Manager settings. These settings are only used for Avaya Equinox® clients.

• **Platform:** The platform settings can be overridden by exception and System Manager settings. These settings are only used for Avaya Equinox® clients.

• **Exceptions:** The Exceptions settings are specific to the System Manager Home location. These settings are only used for Avaya Equinox® clients.

• **Phone Model:** The phone model settings are specific to Avaya Vantage™ endpoints, Avaya J100 Series IP Phones, and 9600 Series IP Deskphones.

**Home location settings**

When a user moves from one geographical location to another, the Home location settings help to identify the location of the user. When the IP address of the calling phone does not match the IP address pattern of any location, Session Manager uses the dial plan rules and Home location settings to complete the call.

On the System Manager web console, you can configure:

- Dial plan rules from **Routing > Dial Patterns.**
- Home location of a user from **Routing > Locations.**

For information about creating location and dial patterns, see *Administering Avaya Aura® Session Manager.*

**Conferencing setting**

Avaya Aura® Device Services auto discovers the following settings from the Avaya Equinox® Conferencing Management during Avaya Equinox® deployment:

- **CONFERENCE_FACTORY_URI**
As an administrator, you can override the values for these settings from the Avaya Aura® Device Services administration portal with any fixed user, group, phone model, or platform value.

### Viewing Home location

**Procedure**

1. On the Home page of the System Manager web console, navigate to User Management > Manage Users.
2. Select a user and click View.
3. In the Communication Profile tab, click the arrow next to the Session Manager Profile section.
   - The system displays the Home location in the Call Routing Settings section.

### Implementation of the dynamic configuration settings

With dynamic configuration, different settings that are common at the user, group, platform, global, phone model, and exceptions levels have different priorities. The administrator must take this into account while creating dynamic configurations.

**Avaya Equinox® clients**

For Avaya Equinox® clients, if the same settings from different levels are applied to a user, the system overrides the settings in the following order:

- System Manager
- Exceptions
- Platform
- User
- Group
- Global
- Custom

For example, if a setting is specified at both the platform and group levels, the system overrides the value with the platform level settings.
Other endpoints and phones
For Avaya J100 Series IP Phones, 9600 Series IP Deskphones, and Avaya Vantage™ endpoints, if the same settings from different levels are applied to a user, the system overrides the settings in the following order:
- Phone Model
- Global

Assigning a group identifier to a phone model

About this task
You must assign a group identifier to each supported phone model so that phones can use Avaya Aura® Device Services automatic configuration functionality. The group identifier is used as a path parameter in a request a phone sends to Avaya Aura® Device Services or the Utility Server hosted on Avaya Aura® Device Services to obtain the 46xxsettings.txt file. For example if you assign 123 to a phone model, then Avaya Aura® Device Services will generate 46xxsettings.txt files for that model in the /var/www/html/123/ directory.

Avaya Aura® Device Services does not generate 46xxsettings.txt files for phone models that have no assigned group identifiers.

Note:
If you change the group identifier for a specific phone model, Avaya Aura® Device Services automatically does the following:
- Creates a new 46xxsettings.txt file for that phone model in the new directory.
- Removes the 46xxsettings.txt file from the previous directory.

Procedure
1. On the Avaya Aura® Device Services web administration portal, navigate to Dynamic Configuration > Device Settings.
2. In the Group ID filed, provide a unique identifier for each phone model.
   A group identifier must be an integer between 0 to 999.
3. Click Save.

Creating a new configuration

About this task
Use this procedure to create a new configuration for users, groups, phone models, or platforms. You can also create a new configuration for exceptions, such as settings specific to System Manager.
Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Dynamic Configuration > Configuration**.

2. In the User, Group, Platform, Global, Phone Model, and Exceptions sections, specify the required settings.

   In the Global section, you can use the New, Edit, and Remove buttons to define custom attributes with a default value, description, and validation template.

3. Click **Save**.

4. In the Save Configuration window, select **Create new configuration** and type a name for the specified configuration.

5. Click **Save**.

   You can view the saved configuration from the Configuration drop-down list.

### Configuration field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Search Criteria</strong></td>
<td></td>
</tr>
<tr>
<td>Configuration</td>
<td>Displays the USER, Group, Platform, Global, and Exceptions settings for the selected configuration.</td>
</tr>
<tr>
<td>User</td>
<td>Displays the Settings configured on SMGR, USER, Group, Platform, Global, and Exceptions settings for the user.</td>
</tr>
<tr>
<td>Group</td>
<td>Displays the Group, Platform, and Global settings for the selected group.</td>
</tr>
<tr>
<td>Phone Model</td>
<td>Displays the Phone Model and Global settings for the selected phone model.</td>
</tr>
<tr>
<td>Platform</td>
<td>Specifies a platform to retrieve the data.</td>
</tr>
<tr>
<td></td>
<td>• iOS</td>
</tr>
<tr>
<td></td>
<td>• Android</td>
</tr>
<tr>
<td></td>
<td>• Windows</td>
</tr>
<tr>
<td></td>
<td>• Mac</td>
</tr>
<tr>
<td>USER, Group, Platform, Global, Phone Model, and Exceptions</td>
<td></td>
</tr>
<tr>
<td>Search</td>
<td>Searches the setting name from the list of settings for the typed search string.</td>
</tr>
<tr>
<td>Include</td>
<td>Includes or excludes the setting.</td>
</tr>
<tr>
<td>Setting</td>
<td>Displays a list of settings.</td>
</tr>
<tr>
<td>Value</td>
<td>Specifies the value that is assigned to a setting.</td>
</tr>
</tbody>
</table>
### Configuration settings

The System Manager specific settings, such as, SIP_CONTROLLER_LIST, SIPDOMAIN, ESMRVR, and PRESENCE_SERVER that are available in the **User**, **Group**, and **Global** settings sections are only for testing the Configuration settings.

**Tip:**

To view the details and associated values of each setting, hover your mouse over the icon that is beside the setting name.

Avaya Equinox® does not support the following settings, but they can be used by other clients:

- CONFIG_SERVER
- CONFIG_SERVER_SECURE_MODE
- ENABLE_PRESENCE

For detailed information about configuration settings, see *Planning for and Administering Avaya Equinox® for Android, iOS, Mac, and Windows*.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovered</td>
<td>The system displays this section for the users. Displays the read-only settings. To edit the values, go to the SMGR configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrieve</td>
<td>Retrieves the settings based on the search criteria.</td>
</tr>
<tr>
<td>Save</td>
<td>Saves a new configuration and overwrites an existing configuration.</td>
</tr>
<tr>
<td>Test</td>
<td>Provides a test URL to test the configuration settings.</td>
</tr>
<tr>
<td>Publish</td>
<td>Publishes the configuration settings.</td>
</tr>
<tr>
<td>Reset</td>
<td>Discards any changes made on the page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the existing configuration settings.</td>
</tr>
<tr>
<td>Import</td>
<td>Uploads configuration settings. You can:</td>
</tr>
<tr>
<td></td>
<td>• Import a 46xxsettings.txt file.</td>
</tr>
<tr>
<td></td>
<td>• Perform a bulk import.</td>
</tr>
<tr>
<td></td>
<td>• Import dynamic configuration settings.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Published Settings</td>
<td>Displays all the published settings for Global, Group, User, Platform, Phone Model, and Exceptions.</td>
</tr>
</tbody>
</table>
### Avaya Aura® Device Services specific parameters

The following table lists Avaya Aura® Device Services specific configuration parameters. For detailed information about other configuration settings, see *Planning for and Administering Avaya Equinox® for Android, iOS, Mac, and Windows*.

#### SIP parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Avaya Equinox® platform support</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMM_ADDR_HANDLE_TYPE</td>
<td>A virtual configuration setting that defines the SIP handle subtype for the user. The SIP handle subtype setting is used to select the correct SIP handle for the Avaya Aura® System Manager users. The system does not send virtual settings to endpoints, and these settings are for the Dynamic Configuration service internal usage only. AutoConfig Service does not respond with SIPUSERNAME and SIPDOMAIN if COMM_ADDR_HANDLE_TYPE is not configured. The options are: • Avaya SIP: Only numeric SIP handles of subtype Avaya SIP are retrieved from System Manager. The system ignores all other alphanumeric SIP handles of Avaya SIP subtype. • Avaya E.164: Maximum 15 digits and a plus (+) prefix are retrieved from System Manager. • Blank: The system rejects the blank value.</td>
<td>Supported only on Avaya Aura® Device Services.</td>
</tr>
<tr>
<td>COMM_ADDR_HANDLE_LENGTH</td>
<td>The parameter that indicates the required length of the Avaya SIP handle for the user. This field is mandatory if you select Avaya SIP for COMM_ADDR_HANDLE_TYPE. Accepted values are 4 to 25.</td>
<td>Supported only on Avaya Aura® Device Services.</td>
</tr>
</tbody>
</table>
Overwriting an existing configuration

About this task

You can overwrite an existing configuration that can be applied to the following: a user, a group, a platform, a phone model, exceptions, and all users.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to Dynamic Configuration > Configuration.
2. In the User, Group, Platform, Global, Phone Model, or Exceptions fields, specify the settings.
3. Click Save.
4. In the Save Configuration window, select Overwrite existing configuration and select an existing configuration.
5. Click Save.

The system overwrites the configuration settings to an existing configuration.

Testing configuration settings

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to Dynamic Configuration > Configuration.
2. In the Configuration field, select a saved configuration.
3. Click Test.

The system displays the Test Settings window.
4. Copy the URL from the Test URL field and paste in a browser to view the changed settings.

You must use the administrator credentials to view the settings.
5. Click OK to close the Test Settings window.
Publishing the configuration settings

About this task

Publish the configuration settings to override the user settings for the specified user, the group settings for the specified group, the platform settings for the specified platform, the phone model settings for the specified model, or all global settings specified.

After publishing the endpoint settings, Avaya Aura® Device Services generates a new 46xxsettings.txt file for the selected endpoint series and stores this file on the Utility Server. The file is stored in the /var/www/html/<endpoint group ID>/ directory, where <endpoint group ID> is the group identifier assigned to the endpoint model. If you publish Global settings, then Avaya Aura® Device Services generates new 46xxsettings.txt files for all supported endpoint series.

If you change the group identifier assigned to an endpoint model, Avaya Aura® Device Services automatically generates a new 46xxsettings.txt file in the /var/www/html/<new endpoint group ID>/ directory.

Important:

• If the Utility Server is disabled, Avaya Aura® Device Services will not generate 46xxsettings.txt files after publishing Global or Phone Model settings.

• If you change the Default Configuration parameters, such as Lock settings, Obscure lock settings, or Split Horizon DNS mapping, you need to republish the Global and Phone Model settings to include these changes to 46xxsettings.txt files.

Before you begin

• If you are publishing Phone Model endpoint settings, make sure that a group identifier is assigned to the required endpoint series on the Device Settings page. Otherwise, Avaya Aura® Device Services does not generate the 46xxsettings.txt file for the selected endpoint series and displays an error message.

Note:

If you are publishing Global settings, Avaya Aura® Device Services generates 46xxsettings.txt files for endpoints with assigned group identifiers only, but does not display any warning messages.

• Test configuration settings before publishing them. For more information, see Testing configuration settings on page 79.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to Dynamic Configuration > Configuration.

2. In the Configuration field, select a saved configuration.

3. At the bottom of the page, click Publish.

   The system displays the Publish/Delete Settings window.

4. To apply the user settings to a user, select the User settings will be applied to user check box and type the name of the user.
5. To apply the group settings to a group, select the **Group settings will be applied to** group check box and from the drop-down list, select the name of the group.

6. To apply the platform settings to a platform, select the **Platform settings will be applied to** check box and from the drop-down list, select the name of the platform.

7. To apply the exception settings, select the **Exceptions will be applied to** check box and from the **Condition** field, click **Home Location**, and from the adjacent field select the location.

8. To apply the endpoint settings to specific endpoint series, select the **Phone model settings will be applied to** check box and from the drop-down list, select the required endpoint series.

9. To apply the global settings to all users, select the **Global settings will be applied to all users** check box.

10. Click **Publish**.

   Based on the publishing settings, the system applies the settings.

---

**Viewing published settings**

**About this task**

Use this procedure to view all the published settings for Global, Group, User, Platform, Phone Model, and Exceptions. You can also delete these settings from the View Published Settings page.

**Procedure**

1. On the Avaya Aura® Device Services web administration portal, navigate to **Dynamic Configuration > Configuration**.

2. Click **View Published Settings**.

3. On the View Published Settings page, from the **Select a Category** list, click one of the following options:
   - All
   - Group
   - User
   - Platform
   - Phone Model
   - Exceptions

4. To view published settings for a specific group, user, platform, phone model, and exception, select the required value from the list, for example, Group Name, to view published settings for a specific group.
You can see the setting name, value of the setting, category, and category value for the selected criteria.

5. To unpublish settings, select the published setting you want to unpublish, and click **Delete Settings**.

---

**Retrieving configuration settings for a user**

**About this task**

Use this procedure to retrieve the configuration settings of a user using the Avaya Aura® Device Services configuration options. If the settings of that user were never changed or published, the system displays a message **Settings not found** in the Group, Platform, and Global settings sections. But you can change the settings of that user by editing and publishing the user settings of another configured user or another Test Configuration.

For example: user1@xyz.com is configured and the administrator wants to update all usernames of user2@xyz.com and publish these settings for user2@xyz.com. The administrator can select the configuration settings of user1@xyz.com and publish the settings for user2@xyz.com.

**Procedure**

1. On the Avaya Aura® Device Services web administration portal, navigate to **Dynamic Configuration > Configuration**.

2. In the **Search Criteria** section, do the following:
   a. Click the **User** check box, and type the name of the user.
   b. In the **Platform** field, click the appropriate platform.
   c. Click **Retrieve**.

   The system displays the configuration settings of the user.

---

**Import of dynamic configuration settings**

**Importing dynamic configuration settings using a file in the JSON format**

**About this task**

Use the following procedures to import configuration settings that are not currently available in Avaya Aura® Device Services. You can perform this task if you need Avaya Equinox® client features with new configuration parameters.
Before you begin
Download and use the additional parameter settings file from PLDS. Ensure that the settings file has the .txt extension and that it is in the JSON format. For example, dynamicConfigUpload.txt.

Procedure
1. On the Avaya Aura® Device Services web administration portal, in the left navigation pane, click Dynamic Configuration > Configuration.
2. On the Configuration page, click Import.
3. On the Import dynamic configuration settings page, in the Select type of import field, select Import dynamic settings.
4. Click Browse and select the settings file that you want to import.
5. Click Import.
The new setting is added in all the existing test configuration at all levels. You can now publish the setting to the required category (Group, User, Platform, Global, Phone Model, or Exception).

Importing parameter values from a 46xxsettings.txt file

About this task
Use this procedure to update the dynamic configuration parameter values stored on Avaya Aura® Device Services with the values from the imported 46xxsettings.txt file. You can choose the settings category that will use these values.

Procedure
1. On the Avaya Aura® Device Services web administration portal, in the left navigation pane, navigate to Dynamic Configuration > Configuration.
2. On the Configuration page, click Import.
4. Click Browse and select the file that you want to import.
5. Click Import.
The system imports the values and displays the results of the import. You can then save or publish the imported values.

Bulk imports
You can add dynamic configuration settings in bulk. You can either import a file from the local system or specify the settings manually. Each setting must be added as a separate line and must
The following table describes bulk settings that you can use:

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CATEGORY</td>
<td>The high-level category to which the particular setting belongs. The categories are:</td>
</tr>
<tr>
<td></td>
<td>• USER</td>
</tr>
<tr>
<td></td>
<td>• GLOBAL</td>
</tr>
<tr>
<td></td>
<td>• GROUP</td>
</tr>
<tr>
<td></td>
<td>• PLATFORM</td>
</tr>
<tr>
<td></td>
<td>• PHONEMODEL</td>
</tr>
<tr>
<td></td>
<td>• EXCEPTION</td>
</tr>
<tr>
<td>{SUB-CATEGORY}</td>
<td>The name or ID of the particular object (user ID, group name, or platform name) for which the setting value will be inserted, updated, or deleted.</td>
</tr>
<tr>
<td></td>
<td>• For the GROUP category, the subcategory is a group name. You can retrieve the group name from LDAP Server.</td>
</tr>
<tr>
<td></td>
<td>For example: GROUP;Group 1;SUPPORTEMAIL;<a href="mailto:admin@mysite.com">admin@mysite.com</a></td>
</tr>
<tr>
<td></td>
<td>• For the USER category, the subcategory is a user name. The setting name is ESMUSERNAME.</td>
</tr>
<tr>
<td></td>
<td>For example: USER;<a href="mailto:user1@mysite.com">user1@mysite.com</a>;CESUSERNAME;<a href="mailto:user1@mysite.com">user1@mysite.com</a></td>
</tr>
<tr>
<td></td>
<td>• For the PLATFORM category, the subcategory is a platform name. The options are Mac, Windows, Android, and iOS.</td>
</tr>
<tr>
<td></td>
<td>For example: PLATFORM;Windows;APPCAST_URL;<a href="https://appcast.mysite.com">https://appcast.mysite.com</a></td>
</tr>
<tr>
<td></td>
<td>• For the PHONEMODEL category, the subcategory is a phone model. The options are J1XX, Vantage, and 96XX.</td>
</tr>
<tr>
<td></td>
<td>For example: PHONEMODEL;J1XX;ADMIN_CHOICE_RINGTONE;Default</td>
</tr>
<tr>
<td></td>
<td>• For the GLOBAL category, there is no subcategory. The format is:</td>
</tr>
<tr>
<td></td>
<td>{CATEGORY};{SETTING_NAME};{SETTING_VALUE}</td>
</tr>
<tr>
<td></td>
<td>For example: GLOBAL;CESSECURE;1</td>
</tr>
<tr>
<td></td>
<td>• For the EXCEPTION category, the format is:</td>
</tr>
<tr>
<td></td>
<td>{CATEGORY};{SOURCE};{EXCEPTION_CONDITION_NAME};{EXCEPTION_CONDITION_VALUE};{SETTING_NAME};{SETTING_VALUE}.</td>
</tr>
</tbody>
</table>
Settings | Description
--- | ---

Where:
- `{SOURCE}` is System Manager.
- `{EXCEPTION_CONDITION_NAME}` is the Home location.
- `{EXCEPTION_CONDITION_VALUE}` is the location name.
- `{SETTING_NAME}` is the name of the setting.
- `{SETTING_VALUE}` is the value of the setting.

For example: `EXCEPTION;SMGR;Home Location;location1;PHNLDLENGTH;5`

Tip:

To delete a setting from the configuration service, append `DELETE` instead of `{SETTING_VALUE}`.

For example: `USER;user1@mYSite.com;CESUSERNAME;DELETE`

**Supported characters for bulk import**

In the bulk import file, you can use the majority of special characters as is. The following are the exceptions:

- To use a semicolon `;`, enclose the entire attribute containing a semicolon with quotation marks.
  
  For example, if you have a group with the name `SEMICON;GROUP`, use the following:
  
  `GROUP;"SEMICON;GROUP";PARAMETER_NAME;parameter_value`

- To use a backslash `\`, prepend it with three backslash characters as follows: `\\\\`

  For example, if you have a group with the name `BACKSLASH\`, use the following:
  
  `GROUP;BACKSLASH\\\\;PARAMETER_NAME;parameter_value`

- To use quotation marks `"`, prepend them with three backslash characters as follows: `\\"`

  For example, if you have a group with the name `QUOTATION_MARKS"`, use the following:
  
  `GROUP;QUOTATION_MARKS\\";PARAMETER_NAME;parameter_value`

- To use the pound sign `#`, prepend it with two backslash characters as follows: `\\#`

  For example, if you have a group with the name `GROUP_WITH_NUMBER_SIGN#`, use the following:

  `GROUP;GROUP_WITH_NUMBER_SIGN\\#;PARAMETER_NAME;parameter_value`

**Importing configuration settings using the bulk import process**

**Before you begin**

If you are importing a `.csv` file created using Microsoft Excel, ensure that the file does not contain any additional characters. To do so, open the file in any other text editor. For example, if you add the string `GROUP;ADMINISTRATORS;SIP_CONTROLLER_LIST;"127.0.0.1:5061;transport=TLS"` using Microsoft Excel and then open the file in a text editor, you will see that the string now
contains some additional quotation marks: "GROUP;ADMINISTRATORS;SIP_CONTROLLER_LIST:"10.255.249.144:5061;transport=TLS"". You must remove any additional characters. Otherwise, bulk import will fail.

**Procedure**

1. On the Avaya Aura® Device Services web administration portal, in the left navigation pane, navigate to **Dynamic Configuration > Configuration**.

2. On the Import dynamic configuration settings page, in the **Select type of import** field, select **Bulk Import**.

3. To import the settings, do one of the following:
   - In the text box, type the required entry on each line in the following format and click **Import**.
     ```
     {CATEGORY}
     ;
     {SUB-CATEGORY}
     ;
     {SETTING_NAME}
     ;
     {SETTING_VALUE}
     ```
   - Click **Browse** to select a file from the local system and click **Import**.

   The file must be in either the .csv or .txt format.

The system displays the import status at the top of the page.

When the import is successful, the system displays a message with the date and time of starting and completing the import. For example: Bulk Import is completed. Started at 2015-12-30 01:01:48. Completed at 2015-12-30 01:01:49

When the import fails, the system displays a message with the reason of the import failure and the List of errors table that has the String number, String, and Error description columns. For example: Bulk Import failed. Reason: Input data validation failed.

**Bulk Import field descriptions**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulk Import Text Box</td>
<td>Specifies the dynamic configuration settings in each line. You can either import a file from the local system by using the <strong>Browse</strong> button or specify the settings manually in this text box. This text box is expandable to add multiple configuration settings.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browse</td>
<td>Enables you to select a file in the .csv format for importing the bulk configuration settings.</td>
</tr>
</tbody>
</table>
Administering the default configuration

About this task
You can maintain internal Dynamic Configuration parameters using the Default page.

Note:
If you are using automatic configuration to provide 46xxsettings.txt files to endpoints, you must republish the Group and Phone Model settings after updating the default configuration settings. Otherwise, 46xxsettings.txt files will not contain the updated configuration parameters.

Procedure
1. On the Avaya Aura® Device Services web administration portal, in the left navigation pane, navigate to Dynamic Configuration > Default.
2. Modify the default configuration settings.
3. Click Save.

Defaults field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow passwords</td>
<td>Specifies that the user can log in to the device with the stored password on the server.</td>
</tr>
<tr>
<td></td>
<td>• If you select the check box, the Dynamic Configuration displays the SIPHA1 and SIPPASSWORD settings. The Avaya UC clients use these SIP credentials for Unified login.</td>
</tr>
<tr>
<td></td>
<td>• If you clear the check box, the Dynamic Configuration does not display the SIPHA1 and SIPPASSWORD settings.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Lock Settings</strong></td>
<td>Specifies that the administrator can lock the attributes. The system displays the locked attributes on the client, but the user cannot edit locked attributes. In the Dynamic Configuration response, the system always displays the LOCKED_PREFERENCES settings that contain the settings that are specified for the user. When you select the <strong>Lock Settings</strong> check box, the system displays the <strong>Obscure locked settings</strong> check box.</td>
</tr>
</tbody>
</table>
| **Obscure locked settings** | Specifies that the all log setting will also be included in the OBSCURE_PREFERENCES setting in the Dynamic Configuration service output.  

- If you select the check box, you can view the obscured settings (OBSCURE_PREFERENCES) in the Dynamic Configuration response.  
The value of OBSCURE_PREFERENCES and LOCKED_PREFERENCES are the same.  
- If you clear the check box, the system hides the obscured settings (OBSCURE_PREFERENCES) in the Dynamic Configuration response.                                                                 |

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Save</strong></td>
<td>Saves the default configuration settings.</td>
</tr>
<tr>
<td><strong>Cancel</strong></td>
<td>Resets any changes made on the page.</td>
</tr>
</tbody>
</table>

### Split Horizon DNS mapping

With Split Horizon DNS mapping, clients can be supported inside and outside the firewall of an enterprise.

The Dynamic Configuration service output contains different settings, such as, ESMSRVR, CESSRVR, DIRSRVR, SIP_CONTROLLER_LIST, CONFERENCE_PARTICIPANT_URL, APPCAST_URL. These settings can contain IP addresses. To replace the IP addresses with appropriate FQDNs for these settings in the Dynamic Configuration service output, enable the Split Horizon DNS mapping feature.

**Note:**

If you are using automatic configuration to provide 46xxsettings.txt files to endpoints, you must republish the Group and Phone Model settings after updating Split Horizon DNS mapping. Otherwise, 46xxsettings.txt files will not contain the updated configuration parameters.
Example

For example, a Presence server is located internally in an enterprise network and also has Network Address Translation (NAT) access from outside the enterprise using the internet. In this case, there will be two Presence server IP addresses for the clients.

For the Presence server, the internal IP address is 190.160.10.1 and external IP address is 90.165.14.11:

- On the Configurations page, you can use any of these two IP addresses as the value for the PRESENCE_SERVER setting.
- FQDN of the Presence server is pserver1.avaya.com.

To configure Split Horizon DNS mapping, you need to map the Presence server IP address to the Presence server FQDN. When you enable Split Horizon DNS mapping, the internal and external clients receive the PRESENCE_SERVER setting with the same value (FQDN): pserver1.avaya.com.

---

Mapping the IP address to the FQDN

About this task

Use this procedure to map the IP address to the FQDN so that the client can connect with the servers or URLs inside and outside the enterprise firewall.

Procedure

1. Log on to the Avaya Aura® Device Services web administration portal.
2. In the left navigation pane, click Dynamic Configuration > DNS Mapping. The system displays the Split Horizon DNS Mapping page.
3. Click Add. The system displays a new row to add the IP address and FQDN.
4. In the IP address field, type the IP address of the server or URL to which the client will connect.
5. In the Fully Qualified Domain Name field, type the FQDN of the server or URL to which the client will connect.
6. Click Save.

---

Enabling Split Horizon DNS mapping

Procedure

1. Log on to the Avaya Aura® Device Services web administration portal.
2. In the left navigation pane, click Dynamic Configuration > DNS Mapping. The system displays the Split Horizon DNS Mapping page.
3. Select the **Enable Split Horizon DNS Mappings** check box.

### Split Horizon DNS Mapping field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Search</strong></td>
<td>Searches the values from the list of entries for the typed search string.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Specifies the IP address of the different servers or URLs to which the client will connect.</td>
</tr>
<tr>
<td><strong>Fully Qualified Domain Name</strong></td>
<td>Specifies the fully qualified domain name of the different servers or URLs to which the client will connect.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add</strong></td>
<td>Displays a row to specify the IP address and FQDN of the different servers or URLs to which the client will connect.</td>
</tr>
<tr>
<td><strong>Save</strong></td>
<td>Saves the added row entry.</td>
</tr>
<tr>
<td><strong>Cancel</strong></td>
<td>Discards any changes made on the page.</td>
</tr>
</tbody>
</table>
Chapter 6: Integrated Windows Authentication administration and management

Integrated Windows Authentication (IWA) enables you to log in to different services with the same credentials. To support IWA, some Avaya Aura® Device Services server administration is required. Users must be able to authenticate to the Avaya Aura® Device Services API using a preexisting authentication to a Windows domain. Avaya Aura® Device Services uses SPNEGO to negotiate authentication with the client and Kerberos to validate the authentication of the client user. User roles are retrieved normally through LDAP.

Use the following sections to complete IWA configuration on the Avaya Aura® Device Services and Active Directory servers. Errors in the setup might cause the authentication to fail. You can enable debug logs to assist with troubleshooting.

🌟 Note:

IWA is only supported if you are using a single authentication directory. The domain of the User Principal Name (UPN) or the authentication domain must be the same as the root domain of the directory. If you are using multiple authentication directories, IWA is disabled.

Authentication prerequisites

You must have the following to set up IWA:

- An Active Directory server.
- A DNS server for the DNS domain of Active Directory.
  
  For information about setting up the DNS server, see Planning for and Administering Avaya Equinox® for Android, iOS, Mac, and Windows.
- A Windows client on the Active Directory domain.
- An Avaya Aura® Device Services server that is resolvable by the DNS.
- A domain user that will be mapped to the Service Principal Name (SPN) of the Avaya Aura® Device Services server.
- Domain users for all individual users.
• Only a single authentication domain is supported and all users must be in the same domain.
• The sAMAccountName attribute must match the user name part of the userPrincipalName attribute.

For example, if the sAMAccountName is jdoe, then the userPrincipalName must use the following format: jdoe@<domain.name>.

• To log in to a computer, the user must enter the user name part of the userPrincipalName configured for that user. The domain must also match the domain part of that user userPrincipalName. The user login name format is <user name><domain>.

For example, if the user has the “jdoe@avaya.com” userPrincipalName, where “avaya” is the domain and “jdoe” is the user name, then the user logs in to a computer using the “avaya\jdoe” account.

⚠️ Important:
The Active Directory, Windows client, and Avaya Aura® Device Services server must resolve each other’s FQDNs. However, they do not need to use the same DNS server or belong to the same zone.

---

### Setting up the Windows Domain Controller

**About this task**

Use this procedure to add the Avaya Aura® Device Services SPN to a domain user on the Windows Domain Controller or the Active Directory server. The SPN must be unique across the domain. To avoid issues with duplicated SPNs, keep track of any SPNs assigned to users.

For detailed information about Domain Controller users, see [https://technet.microsoft.com/en-us-library/cc786438(v=ws.10).aspx](https://technet.microsoft.com/en-us-library/cc786438(v=ws.10).aspx).

⚠️ Important:
Enter all commands exactly as shown in this procedure, and use the following guidelines:

• The host name used to access the Tomcat server must match the host name in the SPN exactly. Otherwise, authentication will fail.

• The server must be part of the local trusted intranet for the client.

• The SPN must be formatted as HTTP/<host name> and must be exactly the same everywhere.

• The port number must not be included in the SPN.

• Only one SPN must be mapped to a domain user.

• The Kerberos realm is always the uppercase equivalent of the DNS domain name. For example, EXAMPLE.COM.

**Procedure**

1. Create a new IWA service account.

   Do not select an account associated with an existing user.
2. If you are using Active Directory 2008 or higher, run the following command to attach the SPN to the domain name:

```bash
setspn -S HTTP/<FRONT-END FQDN> <Domain user login>
```

In the following example, "<FRONT-END FQDN>" is aads.example.com and "<Domain user login>" is aads_spn_user:

```bash
setspn -S HTTP/aads.example.com aads_spn_user
```

⚠️ **Important:**
- If you are using Active Directory 2003, you must use `setspn -A` instead of `setspn -S`.
- When you use `setspn -S`, the Active Directory server searches for other users with the same SPN assigned. If the server finds a duplicated SPN, see step 3 on page 93.

3. **(Optional) To remove a duplicated SPN from another user, run the following command:**

```bash
setspn -d <SPN> <old user>
```

4. Use the following command to generate a `tomcat.keytab` file:

```bash
ktpass /out c:\tomcat.keytab /mapuser <Domain User Login>@<Kerberos realm> /princ HTTP/<FRONT-END FQDN>@<Kerberos realm> /pass +rndPass /crypto all /kvno 0
```

In the following example, `<Domain User Login>` is aads_spn_user, `<Kerberos realm>` is EXAMPLE.COM, and `<FRONT-END FQDN>` is aads.example.com:

```bash
ktpass /out c:\tomcat.keytab /mapuser aads_spn_user@EXAMPLE.COM /princ HTTP/ aads.example.com@EXAMPLE.COM /pass +rndPass /crypto all /kvno 0
```

The `tomcat.keytab` file enables Avaya Aura® Device Services to authenticate against the Kerberos Key Distribution Center (KDC). This file assigns a random password to the user.

5. Transfer the generated `tomcat.keytab` file to the Avaya Aura® Device Services server using the OAMP administration portal.

Since this is a credentials file, handle it securely and delete the original file after this file is imported into the Avaya Aura® Device Services server. You can generate and re-import a new `tomcat.keytab` file anytime.

---

**Windows Domain Controller command descriptions**

Setting up the Windows Domain Controller on page 92 uses the following command values:
Command | Description | Example value
---|---|---
<FRONT—END FQDN> | The REST front host FQDN of the Avaya Aura® Device Services server. This is either the FQDN of the Virtual IP assigned to the cluster (if internal load balancing is used) or the FQDN of the external load balancer, if it is used. | aads.example.com
<Domain user login> | The Windows login ID for the domain user you created. | aads_spn_user
<Kerberos realm> | The domain name for the Kerberos realm. The Kerberos realm is always the uppercase equivalent of the DNS domain name. | EXAMPLE.COM

Setting up IWA on the Avaya Aura® Device Services administration portal

About this task

This procedure describes the changes you must perform on the Avaya Aura® Device Services administration portal to configure IWA.

Procedure

1. On the Avaya Aura® Device Services administration portal, click LDAP Configuration.
2. In the Server Address and Credentials area, do the following:
   a. In the Windows Authentication drop-down menu, select Negotiate.
   b. In the Confirm Action dialog box, click OK.
   c. In UID Attribute ID, type userPrincipalName.
      
      If this field is not set to userPrincipalName, you might encounter license issues and other unpredictable behavior.
   d. Ensure that the other settings are appropriate for the LDAP configuration of your Domain Controller.

   **Important:**

   The LDAP server that you use must be the domain controller with the appropriate Active Directory version as the server type.

3. In the Configuration for Windows Authentication area, complete the following information using the same values you provided when setting up the Windows Domain Controller:
   a. In Service Principal Name (SPN), type HTTP/<FRONT—END FQDN>.
      
      For example, HTTP/aads.example.com.
b. Click **Import** to import the *tomcat.keytab* file transferred from the Windows Domain Controller.

   In cluster deployments, the file is transferred to all nodes in the cluster. An additional option is available to send the file to specific nodes in a cluster.

c. In **Kerberos Realm**, type the Kerberos realm, which is usually in all uppercase letters. For example, *EXAMPLE.COM*.

d. In **DNS Domain**, type the DNS domain of the Domain Controller.

   For example, *example.com*.

e. **(Optional)** Select the **Use SRV Record** check box.

f. **(Optional)** If **Use SRV Record** is not selected, in **KDC FQDN**, type the FQDN of the Domain Controller.

   This value also includes the DNS domain at the end. For example, *ad.example.com*.

g. **(Optional)** In **KDC Port**, retain the default value of 88.

   This field is only visible if **Use SRV Record** is not selected.

h. **(Optional)** In a cluster deployment, click **Send Keytab File** to send the *tomcat.keytab* file you imported in step 3.b on page 95 to a specific node.

   This option is useful if the import to a node failed or if you add a new node to your cluster.

4. Click **Save** to retain the settings and restart the server.

   The settings that you updated are used to generate the files needed to configure the Tomcat JAASRealm and the corresponding Sun JAAS Login module for GSS Bind.
Chapter 7: AWS-specific management options

If you deployed Avaya Aura® Device Services in an Amazon Web Services (AWS) environment, use the following sections to perform AWS-specific management operations. You can perform these management operations anytime.

Updating an existing stack with a new CloudFormation template

About this task
You can apply changes to an existing CloudFormation stack by updating the stack with a newer CloudFormation template. Changes to the stack can include additional nodes, new resources, and new port configuration. The system updates all the objects contained in the stack to match the new settings. Existing EBS volumes and S3 buckets are preserved.

To update an existing single-node stack you must use a new single-node stack template. To update an existing cluster you must use a new multi-node stack template. If you are expanding a cluster, you must already have a cluster with two or more nodes. You cannot expand a single AWS node into an AWS cluster

Before you begin
Generate a new CloudFormation template that matches the application and profile of the existing system but includes the additional resources required. For more information, see the “Creating CloudFormation templates” section in Deploying Avaya Aura® Device Services.

Procedure
1. Sign in to the AWS console.
2. Navigate to Services > Management Tools > CloudFormation.
3. Select the stack to update.
4. Click Actions > Update Stacks.
5. Update the stack using the Update Stack pages.
   You can add an additional CIDR block when going from two to three subnets. Do not change the value of any other stack parameters.
Chapter 8: Monitoring options

Monitoring cluster nodes

About this task

Use this procedure to check network issues with your server and to ensure that all clustered nodes are running properly.

Procedure

1. Log on to the Avaya Aura® Device Services web administration portal.
2. In the left navigation pane, click Cluster Configuration > Cluster Nodes.
   The system displays the Cluster Monitoring and Management page.
3. Check the status of the Avaya Aura® Device Services nodes in the table.
   The table has the following column headers to display the status:
   • Node Address
   • Status
   • Service Status
   • Singleton Services
   Audits that run only on a single node are called singleton services.

Cluster Nodes field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual IP</td>
<td>Displays the virtual IP address and FQDN if a virtual IP address is configured. This is used as a load balancer node.</td>
</tr>
<tr>
<td>Virtual IP Master</td>
<td>Displays the virtual IP and FQDN of the master node if a virtual IP address is configured.</td>
</tr>
<tr>
<td>Virtual IP Backup</td>
<td>Displays the virtual IP and FQDN of the backup node if a virtual IP address is configured.</td>
</tr>
<tr>
<td>Seed Node IP</td>
<td>Displays the IP address and FQDN of the seed node of the cluster.</td>
</tr>
<tr>
<td>Virtual IP Utility Server</td>
<td>Displays the virtual IP address and FQDN of the Utility Server.</td>
</tr>
</tbody>
</table>
Logs and alarms

Log management

The system stores the common log at /opt/Avaya/DeviceServices/<version>/logs/AADS.log.

You can view additional messages at /opt/Avaya/DeviceServices/<version>/tomcat/8.0.24/logs/catalina. These messages can be the logs generated during the start of Avaya Aura® Device Services.

Monitoring the Avaya Aura® Device Services logs

About this task

You can monitor the AADS.log file in run time using the tail command.

Procedure

1. On the SAT terminal, log on to Avaya Aura® Device Services.
2. Run the following command:

   `tail -f /opt/Avaya/DeviceServices/<version>/logs/AADS.log`

   The system displays the logs generated during run time.

Setting up the log level

About this task

Use this procedure to select the level of detail that you want to capture in log files.

Procedure

1. Log on to the Avaya Aura® Device Services web administration portal.
2. In the left navigation pane, click Log Management > Log Level.
   The system displays the Adjust Service Logging Level page.
3. In the Logger field, select one of the following options:
   - Avaya Aura® Device Services Logs: Collects the logs generated by the Avaya Aura® Device Services server.
   - System Logs: Collects all the system logs.
   - All Logs: Collects all server and system logs.
4. In the **Current logging level** field, select one of the following options:
   - **ERROR**: Provides critical server errors.
   - **WARNING (Recommended)**: Provides important but non-critical server messages to understand the current function of the server.
   - **INFO**: Provides information about internal server events and messages.
   - **FINE**: Provides detailed logs. The dynamic configuration and web deployment services use this information for debugging purposes.
   - **FINEST**: Provides very detailed logs on frequent events.

   **Warning:**
   
   The FINE and FINEST logging levels can affect system performance.

5. Click **Save**.

---

**Managing logs**

**About this task**

Use this procedure to adjust log levels and collect log files. Support personnel can use the collected log files to assist with troubleshooting.

**Procedure**

1. On the Avaya Multimedia Messaging web administration portal, navigate to **Logs Management > Log Level**.
2. In the Adjust Service Logging Level area, do the following:
   a. From the **Logger** drop-down menu, select the log type.
   b. From the **Current logging level** drop-down menu, select the level of detail that you want captured in log files.
   c. Click **Save** to apply your changes.
3. In the Collect Logs area, do the following:
   a. **(Optional)** To limit the size of the download, type a number between 1 and 20 in **Number of rotated log files to collect (1–20)**.
      
      This setting specifies the number of files from the log file history to include in the log collection. Leaving this setting empty collects all available logs.
   b. To collect logs for a node, click **Collect** in the corresponding row.
   c. To download the collected logs for a node, click **Download**.
   d. For a cluster, if logs from all the nodes are required, repeat substeps b and c.
Alarms

The alarms that Avaya Aura® Device Services triggers are visible in System Manager.

To begin alarm reporting on System Manager, you must set up SNMP user and target profiles. For more information, see *Administering Avaya Aura® System Manager*.

Table 1: Avaya Aura® Device Services alarms

<table>
<thead>
<tr>
<th>Alarm description</th>
<th>Severity</th>
<th>Event code</th>
<th>SNMP OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>AADS Disk space usage is below critical threshold</td>
<td>critical</td>
<td>OP_AADS-00099</td>
<td>.1.3.6.1.4.1.6889.2.89.0.99</td>
</tr>
<tr>
<td>AADS Disk space usage has reached critical threshold</td>
<td>critical</td>
<td>OP_AADS-00098</td>
<td>.1.3.6.1.4.1.6889.2.89.0.98</td>
</tr>
<tr>
<td>AADS Disk space usage is below warning threshold</td>
<td>minor</td>
<td>OP_AADS-00097</td>
<td>.1.3.6.1.4.1.6889.2.89.0.97</td>
</tr>
<tr>
<td>AADS Disk space usage has reached warning threshold</td>
<td>minor</td>
<td>OP_AADS-00096</td>
<td>.1.3.6.1.4.1.6889.2.89.0.96</td>
</tr>
<tr>
<td>AADS Restore process is successful</td>
<td>major</td>
<td>OP_AADS-00095</td>
<td>.1.3.6.1.4.1.6889.2.89.0.95</td>
</tr>
<tr>
<td>AADS Restore process failed</td>
<td>major</td>
<td>OP_AADS-00094</td>
<td>.1.3.6.1.4.1.6889.2.89.0.94</td>
</tr>
<tr>
<td>AADS Backup process is successful</td>
<td>major</td>
<td>OP_AADS-00093</td>
<td>.1.3.6.1.4.1.6889.2.89.0.93</td>
</tr>
<tr>
<td>AADS Backup process failed</td>
<td>major</td>
<td>OP_AADS-00092</td>
<td>.1.3.6.1.4.1.6889.2.89.0.92</td>
</tr>
<tr>
<td>The associated SM is back up and successfully reachable</td>
<td>critical</td>
<td>OP_AADS-00091</td>
<td>.1.3.6.1.4.1.6889.2.89.0.91</td>
</tr>
<tr>
<td>The associated SM is down and hence not reachable for SMGR</td>
<td>critical</td>
<td>OP_AADS-00090</td>
<td>.1.3.6.1.4.1.6889.2.89.0.90</td>
</tr>
<tr>
<td>AADS Server Node Licenses Threshold cleared</td>
<td>minor</td>
<td>OP_AADS-00089</td>
<td>.1.3.6.1.4.1.6889.2.89.0.89</td>
</tr>
<tr>
<td>AADS Server Node Licenses Threshold reached</td>
<td>minor</td>
<td>OP_AADS-00088</td>
<td>.1.3.6.1.4.1.6889.2.89.0.88</td>
</tr>
<tr>
<td>AADS Server Node Licenses Available</td>
<td>major</td>
<td>OP_AADS-00087</td>
<td>.1.3.6.1.4.1.6889.2.89.0.87</td>
</tr>
<tr>
<td>AADS Server Node Licenses Unavailable</td>
<td>major</td>
<td>OP_AADS-00086</td>
<td>.1.3.6.1.4.1.6889.2.89.0.86</td>
</tr>
<tr>
<td>Alarm description</td>
<td>Severity</td>
<td>Event code</td>
<td>SNMP OID</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>----------</td>
<td>--------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>AADS Multisite Adapter Successfully connected to remote site(s)</td>
<td>major</td>
<td>OP_AADS-00085</td>
<td>.1.3.6.1.4.1.6889.2.89.0.85</td>
</tr>
<tr>
<td>AADS Multisite Adapter Cannot connect to remote site(s)</td>
<td>major</td>
<td>OP_AADS-00084</td>
<td>.1.3.6.1.4.1.6889.2.89.0.84</td>
</tr>
<tr>
<td>DRS is up clearing the alarm</td>
<td>major</td>
<td>OP_AADS-00083</td>
<td>.1.3.6.1.4.1.6889.2.89.0.83</td>
</tr>
<tr>
<td>DRS is failed may be because postgres is down or error in DRS eventing, check if postgres is up and repair the node from SMGR GUI</td>
<td>major</td>
<td>OP_AADS-00082</td>
<td>.1.3.6.1.4.1.6889.2.89.0.82</td>
</tr>
<tr>
<td>Successfully connected to Exchange EWS service using delegate account</td>
<td>major</td>
<td>OP_AADS-00081</td>
<td>.1.3.6.1.4.1.6889.2.89.0.81</td>
</tr>
<tr>
<td>Not able to connect Exchange EWS service using delegate account</td>
<td>major</td>
<td>OP_AADS-00080</td>
<td>.1.3.6.1.4.1.6889.2.89.0.80</td>
</tr>
<tr>
<td>Successfully connected to PPM Web service</td>
<td>major</td>
<td>OP_AADS-00079</td>
<td>.1.3.6.1.4.1.6889.2.89.0.79</td>
</tr>
<tr>
<td>Not able to connect to PPM Web service</td>
<td>major</td>
<td>OP_AADS-00078</td>
<td>.1.3.6.1.4.1.6889.2.89.0.78</td>
</tr>
<tr>
<td>AADS Node Certificate is valid</td>
<td>major</td>
<td>OP_AADS-00077</td>
<td>.1.3.6.1.4.1.6889.2.89.0.77</td>
</tr>
<tr>
<td>AADS Node Certificate is expiring, has expired, or cannot be read</td>
<td>major</td>
<td>OP_AADS-00076</td>
<td>.1.3.6.1.4.1.6889.2.89.0.76</td>
</tr>
<tr>
<td>Synchronized with time server</td>
<td>major</td>
<td>OP_AADS-00075</td>
<td>.1.3.6.1.4.1.6889.2.89.0.75</td>
</tr>
<tr>
<td>Synchronization with time server lost</td>
<td>major</td>
<td>OP_AADS-00074</td>
<td>.1.3.6.1.4.1.6889.2.89.0.74</td>
</tr>
<tr>
<td>AADS Media storage is below critical threshold</td>
<td>critical</td>
<td>OP_AADS-00073</td>
<td>.1.3.6.1.4.1.6889.2.89.0.73</td>
</tr>
<tr>
<td>AADS Media storage has exceeded critical threshold</td>
<td>critical</td>
<td>OP_AADS-00072</td>
<td>.1.3.6.1.4.1.6889.2.89.0.72</td>
</tr>
<tr>
<td>AADS Media storage is below warning threshold</td>
<td>minor</td>
<td>OP_AADS-00071</td>
<td>.1.3.6.1.4.1.6889.2.89.0.71</td>
</tr>
<tr>
<td>AADS Media storage has exceeded warning threshold</td>
<td>minor</td>
<td>OP_AADS-00070</td>
<td>.1.3.6.1.4.1.6889.2.89.0.70</td>
</tr>
<tr>
<td>Alarm description</td>
<td>Severity</td>
<td>Event code</td>
<td>SNMP OID</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>AADS Connection to System Manager LDAP server was restored</td>
<td>major</td>
<td>OP_AADS-00069</td>
<td>.1.3.6.1.4.1.6889.2.89.0.69</td>
</tr>
<tr>
<td>AADS Connection to System Manager LDAP server was lost</td>
<td>major</td>
<td>OP_AADS-00068</td>
<td>.1.3.6.1.4.1.6889.2.89.0.68</td>
</tr>
<tr>
<td>AADS Backup Node released Virtual IP back to Primary</td>
<td>major</td>
<td>OP_AADS-00067</td>
<td>.1.3.6.1.4.1.6889.2.89.0.67</td>
</tr>
<tr>
<td>AADS Backup Node acquired Virtual IP from Primary</td>
<td>major</td>
<td>OP_AADS-00066</td>
<td>.1.3.6.1.4.1.6889.2.89.0.66</td>
</tr>
<tr>
<td>AADS Connection to Remote Domain was restored</td>
<td>major</td>
<td>OP_AADS-00065</td>
<td>.1.3.6.1.4.1.6889.2.89.0.65</td>
</tr>
<tr>
<td>AADS Connection to Remote Domain was lost</td>
<td>major</td>
<td>OP_AADS-00064</td>
<td>.1.3.6.1.4.1.6889.2.89.0.64</td>
</tr>
<tr>
<td>AADS is not operating in License Restricted Mode</td>
<td>critical</td>
<td>OP_AADS-00063</td>
<td>.1.3.6.1.4.1.6889.2.89.0.63</td>
</tr>
<tr>
<td>AADS is operating in License Restricted Mode</td>
<td>critical</td>
<td>OP_AADS-00062</td>
<td>.1.3.6.1.4.1.6889.2.89.0.62</td>
</tr>
<tr>
<td>AADS is not operating in License Error Mode</td>
<td>major</td>
<td>OP_AADS-00061</td>
<td>.1.3.6.1.4.1.6889.2.89.0.61</td>
</tr>
<tr>
<td>AADS is operating in License Error Mode</td>
<td>major</td>
<td>OP_AADS-00060</td>
<td>.1.3.6.1.4.1.6889.2.89.0.60</td>
</tr>
<tr>
<td>AADS JBoss Backend Certificate is valid</td>
<td>major</td>
<td>OP_AADS-00057</td>
<td>.1.3.6.1.4.1.6889.2.89.0.57</td>
</tr>
<tr>
<td>AADS JBoss Backend Certificate is expiring, has expired, or cannot be read</td>
<td>major</td>
<td>OP_AADS-00056</td>
<td>.1.3.6.1.4.1.6889.2.89.0.56</td>
</tr>
<tr>
<td>AADS OAM Certificate is valid</td>
<td>major</td>
<td>OP_AADS-00055</td>
<td>.1.3.6.1.4.1.6889.2.89.0.55</td>
</tr>
<tr>
<td>AADS OAM Certificate is expiring, has expired, or cannot be read</td>
<td>major</td>
<td>OP_AADS-00054</td>
<td>.1.3.6.1.4.1.6889.2.89.0.54</td>
</tr>
<tr>
<td>AADS REST Certificate is valid</td>
<td>major</td>
<td>OP_AADS-00053</td>
<td>.1.3.6.1.4.1.6889.2.89.0.53</td>
</tr>
<tr>
<td>AADS REST Certificate is expiring, has expired, or cannot be read</td>
<td>major</td>
<td>OP_AADS-00052</td>
<td>.1.3.6.1.4.1.6889.2.89.0.52</td>
</tr>
<tr>
<td>AADS Web Service has passed internal testing</td>
<td>major</td>
<td>OP_AADS-00051</td>
<td>.1.3.6.1.4.1.6889.2.89.0.51</td>
</tr>
<tr>
<td>Alarm description</td>
<td>Severity</td>
<td>Event code</td>
<td>SNMP OID</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------------</td>
<td>----------</td>
<td>------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>AADS Web Service has failed internal testing</td>
<td>major</td>
<td>OP_AADS-00050</td>
<td>.1.3.6.1.4.1.6889.2.89.0.50</td>
</tr>
<tr>
<td>AADS HTTP or SIP error code count is below threshold within time period</td>
<td>major</td>
<td>OP_AADS-00049</td>
<td>.1.3.6.1.4.1.6889.2.89.0.49</td>
</tr>
<tr>
<td>AADS HTTP or SIP error code count has exceeded threshold within time period</td>
<td>major</td>
<td>OP_AADS-00048</td>
<td>.1.3.6.1.4.1.6889.2.89.0.48</td>
</tr>
<tr>
<td>AADS Database storage is below critical threshold</td>
<td>critical</td>
<td>OP_AADS-00047</td>
<td>.1.3.6.1.4.1.6889.2.89.0.47</td>
</tr>
<tr>
<td>AADS Database storage has exceeded critical threshold</td>
<td>critical</td>
<td>OP_AADS-00046</td>
<td>.1.3.6.1.4.1.6889.2.89.0.46</td>
</tr>
<tr>
<td>AADS Database storage is below warning threshold</td>
<td>minor</td>
<td>OP_AADS-00045</td>
<td>.1.3.6.1.4.1.6889.2.89.0.45</td>
</tr>
<tr>
<td>AADS Database storage has exceeded warning threshold</td>
<td>minor</td>
<td>OP_AADS-00044</td>
<td>.1.3.6.1.4.1.6889.2.89.0.44</td>
</tr>
<tr>
<td>AADS System memory is below threshold</td>
<td>major</td>
<td>OP_AADS-00043</td>
<td>.1.3.6.1.4.1.6889.2.89.0.43</td>
</tr>
<tr>
<td>AADS System memory is exceeding threshold</td>
<td>major</td>
<td>OP_AADS-00042</td>
<td>.1.3.6.1.4.1.6889.2.89.0.42</td>
</tr>
<tr>
<td>AADS System log level is no longer set to debug, which will improve performance</td>
<td>minor</td>
<td>OP_AADS-00041</td>
<td>.1.3.6.1.4.1.6889.2.89.0.41</td>
</tr>
<tr>
<td>AADS System log level is set to debug, which will degrade performance</td>
<td>minor</td>
<td>OP_AADS-00040</td>
<td>.1.3.6.1.4.1.6889.2.89.0.40</td>
</tr>
<tr>
<td>AADS System load average is below threshold</td>
<td>major</td>
<td>OP_AADS-00037</td>
<td>.1.3.6.1.4.1.6889.2.89.0.37</td>
</tr>
<tr>
<td>AADS System load average is exceeding threshold</td>
<td>major</td>
<td>OP_AADS-00036</td>
<td>.1.3.6.1.4.1.6889.2.89.0.36</td>
</tr>
<tr>
<td>AADS total created accounts is below maximum</td>
<td>major</td>
<td>OP_AADS-00035</td>
<td>.1.3.6.1.4.1.6889.2.89.0.35</td>
</tr>
<tr>
<td>AADS total created accounts has reached maximum</td>
<td>major</td>
<td>OP_AADS-00034</td>
<td>.1.3.6.1.4.1.6889.2.89.0.34</td>
</tr>
<tr>
<td>AADS number of concurrent sessions is below maximum threshold</td>
<td>major</td>
<td>OP_AADS-00033</td>
<td>.1.3.6.1.4.1.6889.2.89.0.33</td>
</tr>
<tr>
<td>AADS number of concurrent sessions is exceeding maximum threshold</td>
<td>major</td>
<td>OP_AADS-00032</td>
<td>.1.3.6.1.4.1.6889.2.89.0.32</td>
</tr>
</tbody>
</table>
## Alarm Description

<table>
<thead>
<tr>
<th>Alarm Description</th>
<th>Severity</th>
<th>Event Code</th>
<th>SNMP OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>AADS rate of requests/responses went below maximum threshold</td>
<td>major</td>
<td>OP_AADS-00031</td>
<td>1.3.6.1.4.1.6889.2.89.0.31</td>
</tr>
<tr>
<td>AADS is exceeding the maximum rate of requests/responses within time period</td>
<td>major</td>
<td>OP_AADS-00030</td>
<td>1.3.6.1.4.1.6889.2.89.0.30</td>
</tr>
<tr>
<td>AADS Connection to Session Manager was restored</td>
<td>major</td>
<td>OP_AADS-00029</td>
<td>1.3.6.1.4.1.6889.2.89.0.29</td>
</tr>
<tr>
<td>AADS Connection to Session Manager was lost</td>
<td>major</td>
<td>OP_AADS-00028</td>
<td>1.3.6.1.4.1.6889.2.89.0.28</td>
</tr>
<tr>
<td>AADS Connection to its Media Store was restored</td>
<td>major</td>
<td>OP_AADS-00027</td>
<td>1.3.6.1.4.1.6889.2.89.0.27</td>
</tr>
<tr>
<td>AADS Connection to its Media Store was lost</td>
<td>major</td>
<td>OP_AADS-00026</td>
<td>1.3.6.1.4.1.6889.2.89.0.26</td>
</tr>
<tr>
<td>AADS Connection to its Data Store was restored</td>
<td>major</td>
<td>OP_AADS-00025</td>
<td>1.3.6.1.4.1.6889.2.89.0.25</td>
</tr>
<tr>
<td>AADS Connection to its Data Store was lost</td>
<td>major</td>
<td>OP_AADS-00024</td>
<td>1.3.6.1.4.1.6889.2.89.0.24</td>
</tr>
<tr>
<td>AADS Connection to LDAP/Active Directory server was restored</td>
<td>major</td>
<td>OP_AADS-00021</td>
<td>1.3.6.1.4.1.6889.2.89.0.21</td>
</tr>
<tr>
<td>AADS Connection to LDAP/Active Directory server was lost</td>
<td>major</td>
<td>OP_AADS-00020</td>
<td>1.3.6.1.4.1.6889.2.89.0.20</td>
</tr>
<tr>
<td>Clear alarm</td>
<td>minor</td>
<td>OP_AADS-00002</td>
<td>1.3.6.1.4.1.6889.2.89.0.2</td>
</tr>
<tr>
<td>An AADS Core Component was restarted successfully</td>
<td>major</td>
<td>OP_AADS-00011</td>
<td>1.3.6.1.4.1.6889.2.89.0.11</td>
</tr>
<tr>
<td>An AADS Core Component has stopped functioning</td>
<td>major</td>
<td>OP_AADS-00010</td>
<td>1.3.6.1.4.1.6889.2.89.0.10</td>
</tr>
<tr>
<td>Test alarm</td>
<td>minor</td>
<td>OP_AADS-00001</td>
<td>1.3.6.1.4.1.6889.2.89.0.1</td>
</tr>
</tbody>
</table>

### Setting up Serviceability Agents for alarms on System Manager

**Before you begin**

Associate the Avaya Aura® Device Services server with the configured Session Manager.

On System Manager, set up an SNMPv3 user profile from Services > Inventory > Manage Serviceability Agents > SNMPv3 User Profiles.

Set up an SNMP target profile from Services > Inventory > Manage Serviceability Agents > SNMP Target Profiles.
About this task
To receive Avaya Aura® Device Services alarms in System Manager, you must set up Serviceability Agents.

Procedure
1. Log on to System Manager.
2. Click Services > Inventory > Manage Serviceability Agents > Serviceability Agents.
3. Select the Avaya Aura® Device Services host name, and click Manage Profiles.
4. Click the SNMP Target Profiles tab.
5. In the Assignable Profiles section, click the SNMP profile you created, and click Assign.
6. Click the SNMPv3 User Profiles tab.
7. In the Assignable Profiles section, select the SNMPv3 profile created, and click Assign.
   System Manager is now ready to receive alarms from Avaya Aura® Device Services.

Enhanced Access Security Gateway for real time support

About this task
Use this procedure to enable Enhanced Access Security Gateway (EASG) functionality in Avaya Aura® Device Services. Avaya support engineers can use this functionality to access your computer and resolve product issues in real time.

The EASG is installed automatically when you deploy the Avaya Aura® Device Services OVA on a VMware standalone host or on vCenter.

Procedure
1. Open the SSH console as an administrator.
2. Check the status of EASG by running the following command:
   ```
   EASGStatus
   ```
   By default, the EASG status is disabled.
3. To enable EASG, run the following command:
   ```
   sudo /usr/sbin/EASGManage --enableEASG
   ```
4. Run the following command to verify the product certificate:
   ```
   sudo EASGProductCert --certInfo
   ```
The system displays the product certificate details.

For example:

```
$ EASGStatus
EASG is disabled
$ sudo /usr/sbin/EASGManage --enableEASG
```

By enabling Avaya Services Logins you are granting Avaya access to your system. This is required to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner.

The product must be registered using the Avaya Global Registration Tool (GRT, see https://grt.avaya.com) to be eligible for Avaya remote connectivity. Please see the Avaya support site (https://support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming.

Do you want to continue [yes/no]? yes

EASG Access is enabled. Performed by user ID: 'admin', on Oct 19 2016 - 12:26

```
$ EASGProductCert --certInfo
Subject: CN= , OU=EASG, O=Avaya Inc.
Serial Number: 10005
Expiration: Aug 6 04:00:00 2031 GMT
Trust Chain:
1. O=Avaya, OU=IT, CN=AvayaITrootCA2
2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2
3. O=Avaya Inc, OU=EASG, CN=EASG Intermediate CA
4. CN=Product EASG Intermediate CA, OU=EASG, O=Avaya Inc.
5. CN= , OU=EASG, O=Avaya Inc.
```

If the certificate expires within 360, 180, 30, or 0 days, the system logs a certificate expiry notification to the `/var/log/messages` file.

---

**Removing EASG**

**About this task**

Use this procedure to remove EASG permanently. You can use the Avaya-provided OVA deployment process to reinstall EASG.

**Procedure**

In the SSH console, run the following command to remove EASG:

```
sudo /opt/Avaya/permanentEASGRemoval.sh
```
Chapter 9: Backup and restore

You can perform backups in a standalone or cluster environment. In case of a system malfunction where one or more Avaya Aura® Device Services nodes must be reinstalled and reconfigured, you can restore the data that was present when you made the backup. The backup and restore procedures are the same, regardless of the deployment method.

The restore procedure must be performed on the same Avaya Aura® Device Services build version from which the backup was made. Patches can cause changes to the format and content of the data that is stored when a backup is taken. Before you restore the data, patch the build to the same patch level that the build was on at the time that the backup was taken.

The backup procedure requires significant resources, so do not perform the backup during busy periods.

Back up Avaya Aura® Device Services

About this task

Use this procedure to back up Avaya Aura® Device Services configuration files and user data. This procedure applies to both standalone and cluster environments. In a cluster environment, you can perform the backup procedure from any node.

Note:

Backing up Avaya Aura® Device Services does not back up the Utility Server data. For more information about backing up data stored on the Utility Server, see Backing up data stored on the Utility Server on page 65.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.

2. Run the following command to create a backup file in TAR format:

   ```
   app backup -t
   ```

3. When prompted with Yes for proceed, all else for cancel, type Yes and then press Enter.

   Avaya Aura® Device Services creates a backup file in the administrator’s home directory. In a cluster environment, backup files are created on each cluster node.

4. Ensure that the administrator’s home directory contains the backup file.
5. Copy the backup files to an external storage using a file transfer program, such as SFTP or SCP.

6. In a cluster environment, repeat steps 4 and 5 on all remaining nodes in the cluster.

---

**Restoring options for standalone and cluster environments**

**Restoring Avaya Aura® Device Services in a standalone environment**

**About this task**

Use this procedure to restore a standalone Avaya Aura® Device Services node.

**Before you begin**

- Ensure that the application installation binary required to install Avaya Aura® Device Services is available.

  ✅ **Note:**
  
  The application installer must be the same version as the Avaya Aura® Device Services version that was used to create the backup.

- If the virtual machine needs to be re-created, ensure that the OVA required to deploy the virtual machine is available.

- Ensure that the required Avaya Aura® Device Services backup file is available.

- Determine if the Utility Server was enabled on the system that you are restoring.

**Procedure**

1. Reinstall the same version of Avaya Aura® Device Services that was backed up:
   
   a. Redeploy the OVA if the node needs to be re-imaged.

      For more information about deploying OVAs, see the “Initial setup” section in *Deploying Avaya Aura® Device Services*.

   b. Log in to the Avaya Aura® Device Services CLI as an administrator and run the following command:

      ```
      app install
      ```

   c. If the Utility Server was enabled on the system that you are restoring, enable the Utility Server from the **Utility Server** menu.
d. In the **Front-end host, System Manager and Certificate Configuration** menu, configure the following settings:

- System Manager FQDN
- System Manager Enrollment Password
- Keystore password

e. In the **Session Manager Configuration** menu, configure the following settings:

- Session Manager Management IP
- Session Manager Asset IP

f. After the initial setup is completed, run the Configuration Utility using the `app configure` command.

g. If the Utility Server was enabled on the system that you are restoring, in the **Utility Server Configuration** menu, configure the following settings:

- Utility Server VIP
- Utility Server FQDN

2. Copy the backup file to the home directory of the administrative user using a file transfer utility, such as SFTP or SCP.

3. Run the following command to set the ownership of the backup file:

   ```bash
   sudo chown -R ucapp:ucgrp <path>
   ```
   
   In this command, `<path>` is the absolute path to the backup file.

4. Run the following command to restore the backup file:

   ```bash
   app restore <path>
   ```
   
   In this command, `<path>` is the absolute path to the backup file.

**Next steps**

If the Utility Server is enabled on the system and you need to restore Utility Server data, see *Restoring the Utility Server data* on page 66.

---

**Restoring an Avaya Aura® Device Services cluster**

**About this task**

Use this procedure to restore an entire cluster. Restoring a cluster is useful if a failure occurs that results in the loss of all nodes.

To restore an Avaya Aura® Device Services node, you must install the Avaya Aura® Device Services software, then restore the configuration and data files from a previously made backup.

**Before you begin**

- Ensure that the application installation binary required to install Avaya Aura® Device Services is available.
Note:

The application installer must be the same version as the Avaya Aura® Device Services version that was used to create the backup.

• If the virtual machine needs to be re-created, ensure that the OVA required to deploy the virtual machine is available.

• Ensure that the required Avaya Aura® Device Services backup files are available for the nodes that are restored. Each node has its own specific backup file. When restoring an Avaya Aura® Device Services node, you must use the correct backup file for that node.

• Determine if the Utility Server was enabled on the system that you are restoring.

Procedure

Perform step 1 on the seed node first, and then on all non-seed nodes.

1. Reinstall the same version of Avaya Aura® Device Services that was backed up:
   a. Redeploy the OVA if the node needs to be re-imaged.
      For more information about deploying OVAs, see the “Initial setup” section in Deploying Avaya Aura® Device Services.
   b. Log in to the Avaya Aura® Device Services CLI as an administrator and run the following command:
      
      ```
      app install
      ```
   c. If the Utility Server was enabled on the system that you are restoring, enable the Utility Server from the Utility Server menu.
   d. If you are reinstalling a non-seed node, in the Cluster Configuration menu, set Initial cluster node to n.
   e. If you are reinstalling a non-seed node, in the Cluster Configuration menu, set Cluster seed node to the IP address of the seed node.
   f. In the Front-end host, System Manager and Certificate Configuration menu, configure the following settings:
      • System Manager FQDN
      • System Manager Enrollment Password
      • Keystore password
   g. In the Session Manager Configuration menu, configure the following settings:
      • Session Manager Management IP
      • Session Manager Asset IP
   h. After the initial setup is completed, run the Configuration Utility using the app configure command.
   i. If you enabled the Utility Server, configure the settings in the Clustering Configuration menu.
j. If the Utility Server was enabled on the system that you are restoring, in the Utility Server Configuration menu, configure the following settings:

- Utility Server VIP
- Utility Server FQDN

Perform steps 2 to 4 on the seed node first and then on all non-seed nodes.

2. Copy the backup file to the home directory of the administrative user using a file transfer utility, such as SFTP or SCP.

   Ensure that you are using the backup file created for the current node.

3. Run the following command to set the ownership of the backup file:

   ```bash
   sudo chown -R ucapp:ucgrp <path>
   ```

   In this command, `<path>` is the absolute path to the backup file.

4. Run the following command to restore the backup file:

   ```bash
   app restore <path>
   ```

   In this command, `<path>` is the absolute path to the backup file.

5. From the seed node, run the following command to repair the Cassandra database:

   ```bash
   sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/cassandra/
   cassandraRepair.sh -M
   ```

   If prompted, enter the Cassandra database user name and password. The default Cassandra database user name and password are `aem_system` and `avaya123` respectively.

**Next steps**

If the Utility Server is enabled on the system and you need to restore Utility Server data, see Restoring the Utility Server data on page 66.
Chapter 10: Avaya Aura® Device Services upgrade operations

The upgrade path can flow through one or more prior releases, depending on the currently installed release. The following table shows the specific release upgrades along the upgrade path.

<table>
<thead>
<tr>
<th>Upgrade path number</th>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7.0.1.2</td>
<td>7.1</td>
</tr>
<tr>
<td>2</td>
<td>7.1</td>
<td>7.1.2</td>
</tr>
<tr>
<td>3</td>
<td>7.1.2</td>
<td>7.1.3</td>
</tr>
<tr>
<td>4</td>
<td>7.1.2</td>
<td>7.1.3 SP1</td>
</tr>
<tr>
<td>5</td>
<td>7.1.3</td>
<td>7.1.3 SP1</td>
</tr>
<tr>
<td>6</td>
<td>7.1.3 SP1</td>
<td>7.1.3 SP2</td>
</tr>
<tr>
<td>7</td>
<td>7.1.3. SP2</td>
<td>7.1.5</td>
</tr>
<tr>
<td>8</td>
<td>7.1.5</td>
<td>7.1.6</td>
</tr>
</tbody>
</table>

Depending on the release you are currently using, you might need to perform several upgrade procedures. For example, if you want to upgrade Avaya Aura® Device Services Release 7.1.3 SP1 to Release 7.1.6, follow upgrade paths 6, 7, and 8.

This document focuses on the upgrade process for path 8. For information about migration and upgrade processes for previous releases, see the following documents:

- For Release 7.1, see “Upgrading Avaya Aura® Device Services” in Deploying Avaya Aura Device Services.
- For Release 7.1.2, see “Upgrades and migrations” in Administering Avaya Aura Device Services.
- For Release 7.1.3.x, see “Avaya Aura® Device Services upgrade operations” in Administering Avaya Aura Device Services.
- For Release 7.1.5, see “Avaya Aura® Device Services upgrade and migration operations” in Administering Avaya Aura Device Services.

**Important:**

Perform the system layer update before you upgrade Avaya Aura® Device Services.
System layer (OS) updates for virtual machines deployed using Avaya-provided OVAs

Each VMware or AWS virtual machine that is created by deploying the Avaya Aura® Device Services OVA file has a system layer (operating system). The system later is updated with system layer updates provided by Avaya.

⚠️ Important:

Do not apply updates obtained from sources other than Avaya to the system layer of Avaya Aura® Device Services virtual machines. Only use update artifacts provided by Avaya.

This section only applies to systems deployed in VMware or AWS virtual environments using Avaya-provided OVAs. As the customer, you are responsible for updating the operating system when Avaya Aura® Device Services is installed as a software-only application onto, using update artifacts from Red Hat.

The process to install a system layer update involves the following steps:

- Determine if the system layer update is applicable to the given virtual machine. If the update is not applicable, then there is no action required.
- Download, extract, and stage the update.
- Install the update during a maintenance window.

Determining if a system update is applicable

About this task

Before installing a system update for a virtual machine, query the version of the currently installed system. Use the current version to determine if the system layer requires an update. It is possible that the machine was installed using an OVA that was already built with the latest system layer version.

Procedure

1. Log in to the virtual machine using the administrative user id.
2. Query the version number of the system version by running the `sys versions` command.

🌟 Note:

The patch level reported by the above command is not used at this time, and is to be ignored.

Next steps

If the above system version is already on the recommended system update, then no further action is required.
If the above system version is lower than the recommended system update version, then continue with the process to download and stage the update.

---

**Downloading, extracting, and staging a system layer update**

**About this task**

Before installing a system layer update, you must first download the update from the Avaya support site, and then extract and stage the update on the system. The staging process places the update into a system area, which prepares the system for installation of the update.

**Procedure**

1. Download the update from the Avaya Support web site.
   
   `ucapp-system-3.5.0.0.9.tgz` is an example of a system layer update artifact.

2. Transfer the update to the administrative account of the server to be updated, using standard file transfer methods, such as SFTP or SCP.

3. Log in to the administrative account of the server using SSH.

4. To extract the update, use the following command:
   
   ```
   tar -zxf ucapp-system-<version>.tgz
   ```

   For example:
   
   ```
   tar -zxf ucapp-system-3.5.0.0.9.tgz
   ```

5. To stage the update, change to the required directory and perform the following staging command:
   
   ```
   cd ucapp-system-<version>
   sudo ./update.sh --stage
   ```

   For example:
   
   ```
   cd ucapp-system-3.5.0.0.9
   sudo ./update.sh --stage
   ```

6. **(Optional)** To free up disk space, clean up the downloaded and extracted files using the following commands:
   
   ```
   cd..
   rm ucapp-system-<version>.tgz
   rm -rf ucapp-system-<version>
   ```

   For example:
   
   ```
   rm ucapp-system-3.5.0.0.9.tgz
   rm -rf ucapp-system-3.5.0.0.9
   ```

   **Tip:**

   Avaya recommends to clean up the downloaded and extracted artifacts after staging. The staging operation copies the content to an internal system area. The downloaded and extracted content are no longer required.
7. To verify that the update has been staged, query the status:

\[ \text{sysUpdate --status} \]

**Note:**

The `sysUpdate` command is added to the system the first time a system update is staged. After staging, if the command is not recognized, you must exit the current session and establish a new session. Establishing a new session creates the `sysUpdate` command (alias) for the new session.

**Tip:**

If a system update is staged in error, the staged update can be deleted as follows. It is not possible to delete a staged update once the installation of the update has started.

\[ \text{sysUpdate --delete} \]

For additional help with the `sysUpdate` command, use one of the following commands. The `--help` option provides command line syntax. The `--hhelp` option provides verbose help.

\[ \text{sysUpdate --help} \]
\[ \text{sysUpdate --hhelp} \]

**Next steps**

Install the staged update during a maintenance window.

---

### Installing a staged system layer update

**About this task**

After a system update is staged, it can then be installed. The installation runs in the background in order to minimize the possibility of interference, such as the loss of an SSH session. The background installation process follows these steps:

- A login warning message is created so users logging into the system know that a system update is in progress.
- If the application is running, it is shut down.
- The update is installed onto the system.
- The server is rebooted.
- Post-reboot cleanup actions are performed.
- The application is started.
- The login warning message is removed.

**Important:**

Do not perform any system maintenance actions, such as starting, stopping, or upgrading the application, while the system update is in progress.
Procedure

1. Log in to the administrative account using SSH.
2. Type `sysUpdate --install` to start the installation

**Tip:**

The progress of the update can be monitored using one of the following commands. The first command uses the Linux tail browser, whereas the second uses the Linux less browser.

```
sysUpdate --monitor
sysUpdate --monitor less
```

The status of the update can be queried using the command:

```
sysUpdate --status
```

You can obtain logs of the current, and previous, system layer update installations, by using the following command. This command places a zip file of the logs in the current working directory.

```
sysUpdate --logs
```

---

# Upgrading Avaya Aura® Device Services on AVP

**About this task**

The following are the high-level steps for upgrading Avaya Aura® Device Services to Release 7.1.6 when Avaya Aura® Device Services is installed on an Appliance Virtualization Platform (AVP) host.

The following procedures reference clusters. If you are working with a standalone Avaya Aura® Device Services server, ignore the references to other cluster nodes.

**Important:**

- You must use the original host name and IP address from the currently installed cluster when deploying OVAs.
- The upgrade procedure backs up Session Manager Data Storage and restores this data when you perform the rollback procedure. Any Session Manager data that is changed between these two points in time will be lost when you restore this data as part of the rollback procedure. Therefore, Avaya recommends that you avoid configuring or performing any maintenance activities on Session Manager until the completion of either the Avaya Aura® Device Services upgrade procedure or the rollback procedure.

**Procedure**

1. Prepare for the upgrade:
   a. Record the currently installed version of the Avaya Aura® Device Services application.
b. Obtain a copy of that application installer and copy of the OVA for the currently installed release.

c. Obtain a copy of the latest system layer update file, application installer file, and OVA.

d. Back up the Session Manager User Data Storage. This backup is used if you need to abort the upgrade procedure and roll back to the currently installed release.

e. Back up each node of the Avaya Aura® Device Services cluster. These backups are used if you need to abort the upgrade procedure and roll back to the currently installed release.

f. Record configuration values from the existing Avaya Aura® Device Services system.

g. Copy logs, home directory content, and backup files to an external storage.

⚠️ **Important:**

Complete the upgrade preparation steps before the maintenance window, so you can start the upgrade as soon as the maintenance window starts.

2. Upgrade the existing virtual machines:

   a. Upgrade the system layer.

   b. Upgrade the application.

   c. Back up each node of the Avaya Aura® Device Services cluster. These backups are used in the upgrade procedure.

3. Deploy new virtual machines:

   a. Delete the existing virtual machines of the cluster.

   b. Deploy the new Avaya Aura® Device Services Release 7.1.6 OVA to create new virtual machines for each node in the cluster.

4. Restore the Avaya Aura® Device Services Release 7.1.6 application using the backups created in step 2.

   You can also enable the Utility Server.

5. **(Optional)** Migrate the Utility Server data:

   a. Create “no firmware” backups on a legacy 7.1 Utility Services server.

   b. Restore the backup on the Utility Server embedded within the Avaya Aura® Device Services on each cluster node.

6. **(Optional)** If required, you can abort the upgrade procedure and roll back to the previously installed release:

   a. Delete the newly deployed machines of the cluster.

   b. Restore the Session Manager User Data Storage, which was backed up in step 1.

   c. Restore the cluster.
Preparing for an AVP upgrade

About this task
Use this procedure to download the latest installation files required for the upgrade and to collect data from the existing Avaya Aura® Device Services servers to upgrade to the new Avaya Aura® Device Services release.

Perform the upgrade preparation procedure before the maintenance window so you can start the upgrade as soon as the maintenance window starts. This procedure does not alter the system and Avaya Aura® Device Services remains available.

Before you begin
Determine the keystore password you want to use when installing Avaya Aura® Device Services Release 7.1.6.

Procedure
1. Record the currently installed version of the Avaya Aura® Device Services application.
   To upgrade to Release 7.1.6, you must have Avaya Aura® Device Services Release 7.1.5.
2. Back up the cluster as described in Backing up Avaya Aura Device Services on page 107.
   Note: When you create backup files for cluster nodes, you can specify a name for each backup file to keep the backup files organized. For example, if the server host name is server1.example.com, then the app backup -t -d /home/admin recover command creates the /home/admin/recover_server1.tar backup file.
3. Download the application installer file and the OVA file of the same version that is used in the currently installed release.
   You can use these files in case the upgrade is aborted and you need to revert Avaya Aura® Device Services back to the currently installed version.
4. Download the latest versions of the following files:
   - System layer update file.
   - Application installer file.
   - OVA file.
   For more information about system layer updates, see Preparing for an AVP upgrade on page 118.
5. Log in to Avaya Aura® Device Services as an administrative user using an SSH connection.
6. Run the following command to collect the current system logs:
   
   ```
   app collectlogs collect
   ```
Avaya Aura® Device Services creates a `.zip` file containing the logs in the `/var/log/Avaya/collected-logs` directory.

**Note:**
Support teams can resolve issues that might occur on the new system by comparing the collected logs to the logs on the new system.

7. Do the following to record server information and then save the output in a safe location:
   a. To obtain the fully qualified host name, run the following command:
      ```
      hostname -f
      ```
   b. To obtain the IP address and the network mask, run the following command:
      ```
      ifconfig -a | grep inet | grep -v 127.0.0.1
      ```
   c. To obtain the IP address of the default gateway, run the following command:
      ```
      netstat -nrv | grep '^0.0.0.0'
      ```
   d. To obtain the DNS search list and DNS server IP address, run the following command:
      ```
      cat /etc/resolv.conf
      ```
   e. To obtain the NTP server IP address, run the following command:
      ```
      cat /etc/ntp.conf | grep "^server"
      ```
   f. Log in as the administrator and run the following commands to display the user name and primary group for the administrative account:
      ```
      id --user --name
      id --group --name
      ```
   g. If you want to use the same keystore password, obtain the existing keystore password by referencing notes from the original installation.
      
      If you do not want to use the same keystore password, record a new keystore password.
   h. Record the current System Manager enrollment password by referencing notes from the original installation.

8. Copy the following files to an off-board storage location using a file transfer program, such as SFTP or SCP:
   - The `.zip` archive containing the logs.
   - Any other desired content from the `/home` directory.

9. For each virtual machine in the cluster, record the network to which the virtual machine is attached, and use the original installation notes to record the OVA profile used while deploying the original OVA.

10. Repeat steps 5 to 9 for all remaining nodes in the cluster.

**Next steps**
Upgrade the existing AVP virtual machines.
Upgrading the existing AVP virtual machines

About this task

Use this procedure to upgrade the Avaya Aura® Device Services system layer and application on the existing cluster nodes. This procedure prepares the servers for creating backup files that are later used to restore into newly deployed virtual machines that are deployed using Release 7.1.6 OVAs.

Before you begin

- Ensure that you have created system backups and saved the required server information by completing the upgrade preparation procedure. For more information, see Preparing for an AVP upgrade on page 118.
- Ensure that you have the latest system layer update file and latest binary installer file.
- Upgrade to the latest system layer release on all nodes. For more information, see System layer (OS) updates for virtual machines deployed using Avaya-provided OVAs on page 113.

Important:

You must apply the system layer update to all nodes in the cluster before starting the upgrade process. Otherwise, the upgrade will fail.

- Determine whether you need to enable the Utility Server.

Procedure

1. Log in to the seed node as an administrator using an SSH connection.
2. Run the following command to remove the inactive Avaya Aura® Device Services version:
   ```
   app removeinactive
   ```
3. Transfer the binary file to the administrator’s home directory on the Avaya Aura® Device Services server by using a file transfer tool of your choice.
4. Run the following command to make the file executable:
   ```
   sudo chmod 755 aads-<version>.bin
   ```
   For example:
   ```
   sudo chmod 755  aads-7.1.6.0.16.bin
   ```
5. Run the following command to start the upgrade:
   ```
   sudo ./aads-<version>.bin
   ```
   For example:
   ```
   sudo ./aads-7.1.6.0.16.bin
   ```
6. When the system prompts you to enable the Utility Server, do one of the following:
   - If want to enable the Utility Server, select Yes.
   - If you do not want to enable the Utility Server, select No.
Important:

You must either enable the Utility Server on all nodes or leave it disabled on all nodes.
You cannot enable the Utility Server on some cluster nodes and disable it on other nodes.

7. Follow the system prompts to complete the upgrade procedure.
8. Repeat the steps above on the backup node first, and then on all other non-seed nodes in
   the cluster.
9. Log in to the seed node as an administrative user using an SSH connection.
10. Run the `svc aads start` command to start Avaya Aura® Device Services.
11. Repeat steps 9 and 10 on all other cluster nodes.
12. Verify that DRS replication is working for all nodes on System Manager.
   For more information, see Checking for DRS synchronization on page 131.
13. Log in to the seed node as an administrative user using an SSH connection.
14. Run the following command to create a backup:

```
app backup -t -d <home-directory-of-admin-user> upgrade
```

   The system creates a file with the `upgrade_<hostname>.tar` name in the administrative
   user’s home directory.
15. Run the following command to add permissions to the backup file:

```
sudo chown admin:admingrp upgrade_<hostname>.tar
```
16. Transfer the backup file to an off-board storage location using a file transfer program, such
    as SFTP or SCP.
17. Repeat steps 13 to 16 for all other cluster nodes.

Next steps

Deploy new AVP virtual machines.

Deploying new AVP virtual machines

About this task

Use this procedure to deploy and prepare Release 7.1.6 virtual machines to complete the
upgrade. To improve efficiency, you can perform many steps simultaneously across all nodes in
the cluster.

Before you begin

- Upgrade the existing AVP virtual machines.
- Ensure that you have the latest Avaya Aura® Device Services installer and OVA.
Procedure

1. Log in to the seed node of the existing cluster as an administrative user using an SSH connection.

2. Run the following command on each node in the cluster to stop Avaya Aura® Device Services and verify that the services are stopped:

   ```
svc aads stop
svc aads status
```

3. Run the following command to shut down the Avaya Aura® Device Services Release 7.1.6 virtual machine and turn off the power:

   ```
sudo shutdown -hP now
```

4. Repeat the steps above for all other cluster nodes.

5. Do the following to deploy the Avaya Aura® Device Services Release 7.1.6 OVA:
   a. Delete the existing virtual machine for the seed node.
   b. Deploy the Avaya Aura® Device Services OVA for the seed node.
   c. Configure the new server with the server configuration information you saved from the node.

      For more information, see Preparing for an AVP upgrade on page 118.
   d. Attach the new virtual machine to the network recorded for the node in Preparing for an AVP upgrade on page 118.
   e. Repeat substeps a to d for other cluster nodes.

6. If you have an installer that is newer than the one staged in /opt/Avaya/ within the virtual machine, do the following for each node in the cluster:
   a. Copy the installer to the administrative user’s home directory using a file transfer program, such as SFTP or SCP.
   b. Run the following commands to move the installer to the standard staging location:

      ```
sudo mv aads-<new-release>.bin /opt/Avaya
sudo chown ucapp:ucgrp /opt/Avaya/aads-<new-release>.bin
sudo chmod 750 /opt/Avaya/aads-<new-release>.bin
```
   c. Run the following command to remove the older installer file staged in the virtual machine:

      ```
sudo rm /opt/Avaya/aads-<version-to-be-deleted>.bin
```

Next steps
Complete the upgrade.

Completing the upgrade

About this task

Use this procedure to complete the upgrade of Avaya Aura® Device Services to Release 7.1.6.
Before you begin

- Deploy the new AVP virtual machines.
- Ensure that the required Session Manager and System Manager servers are running and reachable.
- Ensure that you are using the same Avaya Aura® Device Services installer that was used for upgrading the existing AVP virtual machines.

Procedure

1. For each node in the cluster, transfer the backup file that you created when performing Upgrading the existing AVP virtual machines on page 120 to the administrative user’s home directory.
   
   Use a file transfer program, such as SFTP or SCP.

2. For each node in the cluster, transfer the Avaya Aura® Device Services installer, which was used for upgrading the existing AVP virtual machines, to the administrative user’s home directory.

3. Restore the cluster as described in Restoring an Avaya Aura Device Services cluster on page 109.

Next steps

If the Utility Server is enabled on the system, and if you need to migrate the data from a legacy 7.1 Utility Services machine, complete Migrating Utility Server data on page 128.

---

Rolling back the AVP upgrade

About this task

Use this procedure to abort the upgrade procedure and roll back to the previously installed Avaya Aura® Device Services release. Since you can upgrade to 7.1.6 from Release 7.1.5, you can roll back to that release.

Based on the state of the system at the time when you decided to roll back to the previous release, some steps in this procedure might not apply. For example, if the Avaya Aura® Device Services application is not running on a node, then the instructions to stop the node do not apply.

Before you begin

- Complete Preparing for an AVP upgrade on page 118.
- Ensure that the required Session Manager and System Manager servers are running and reachable.

Procedure

1. Log in to the seed node as an administrative user using an SSH connection.

2. Run the following command to stop Avaya Aura® Device Services Release 7.1.6 and verify that the services are stopped:

```
svc aads stop
svc aads status
```
3. Run the following command to shut down the Avaya Aura® Device Services Release 7.1.6 virtual machine and turn off the power:

```bash
sudo shutdown -hP now
```

4. Repeat the steps above for all other cluster nodes.

5. Do the following to deploy the Avaya Aura® Device Services OVA for the previously installed release:
   a. Delete the existing virtual machine for the seed node.
   b. Deploy the Avaya Aura® Device Services OVA for the seed node.
      Use the OVA that you obtained while performing Preparing for an AVP upgrade on page 118.
   c. Configure the new server with the server configuration information you saved from the node while performing Preparing for an AVP upgrade on page 118.
   d. Attach the new virtual machine to the network recorded for the node.
      You obtained this information while performing Preparing for an AVP upgrade on page 118.
   e. Repeat steps a to d for other cluster nodes.

6. If the application installer for the previously installed release is older than the one embedded in the OVA that you used to deploy the virtual machine, do the following for each node in the cluster:
   a. Copy the installer to the administrative user’s home directory using a file transfer program, such as SFTP or SCP.
   b. Run the following commands to move the installer to the standard staging location:
      ```bash
      sudo mv aads-<new-release>.bin /opt/Avaya
      sudo chown ucapp:ucgrp /opt/Avaya/aads-<new-release>.bin
      sudo chmod 750 /opt/Avaya/aads-<new-release>.bin
      ```
   c. Run the following command to remove the older installer file staged in the virtual machine:
      ```bash
      sudo rm /opt/Avaya/aads-<version-to-be-deleted>.bin
      ```

7. On the Home page of the System Manager web console, navigate to **Elements > Session Manager > System Status > User Data Storage**.

8. Click **Backup and Restore**.

9. Select the Session Manager on which you want to run the restore operation.

10. Click **Restore**.

11. From the “Restore File” column, select the backup that you created while performing Preparing for an AVP upgrade on page 118.

12. Do one of the following:
   - Click **Commit** to accept the selection.
13. Click **Confirm** to send a request to each Session Manager to begin the restore operation using the selected file.

   To cancel the restore request, click **Cancel**.

14. Restore the Avaya Aura® Device Services cluster as described in [Restoring an Avaya Aura Device Services cluster](#) on page 109.

---

### Upgrading Avaya Aura® Device Services on ESXi or AWS

**About this task**

The following are the high-level steps for upgrading Avaya Aura® Device Services to Release 7.1.6 when Avaya Aura® Device Services is installed on an ESXi host or an Amazon Machine Image (AMI) in the Amazon Web Services (AWS) cloud environment.

**Note:**

If required, you can abort the upgrade procedure and roll back to the previously installed release.

**Procedure**

1. Obtain a copy of the latest system layer update file and application installer file.
   
   For more information about system layer updates, see [Preparing for an AVP upgrade](#) on page 118.

2. Perform a full system backup.

3. Upgrade the virtual machines:
   
   a. Upgrade the system layer.

   b. Upgrade the Avaya Aura® Device Services application.

4. *(Optional)* Migrate the Utility Services data:
   
   a. Create “no firmware” backups on the legacy 7.1 Utility Services server.

   b. Restore the backup onto each Avaya Aura® Device Services node.

---

### Creating a full system backup

**About this task**

Create a full Avaya Aura® Device Services backup before performing complex maintenance procedures, such as upgrades. If Avaya Aura® Device Services is backed up, you can abort the upgrade procedure and roll back to the previously installed release if required.
Before you begin
Ensure that you are using Avaya Aura® Device Services Release 7.1.5.

Procedure
Complete Backing up Avaya Aura Device Services on page 107.

Next steps
Upgrade ESXi and AWS virtual machines.

Upgrading ESXi or AWS virtual machines

About this task
Use this procedure to upgrade the Avaya Aura® Device Services system and application layers on the existing servers.

Before you begin

• Download the system layer update file and the latest binary installer file.
• Upgrade to the latest system layer release on all nodes. For more information, see System layer (OS) updates for virtual machines deployed using Avaya-provided OVAs on page 113.

Important:
You must apply the system layer update to all nodes in the cluster before starting the upgrade process. Otherwise, the upgrade will fail.
• Determine whether you need to enable the Utility Server.

Procedure
1. Log in to the seed node as an administrator using an SSH connection.
2. Run the following command to remove the inactive Avaya Aura® Device Services version:
   ```bash
   app removeinactive
   ```
3. Transfer the binary file to the administrator home folder on Avaya Aura® Device Services by using a file transfer tool of your choice.
4. Run the following command to make the file executable:
   ```bash
   sudo chmod 755 aads-<version>.bin
   ```
   For example:
   ```bash
   sudo chmod 755 aads-7.1.6.0.16.bin
   ```
5. Run the following command to start the upgrade:
   ```bash
   sudo ./aads-<version>.bin
   ```
   For example:
   ```bash
   sudo ./aads-7.1.6.0.16.bin
   ```
6. When the system prompts you to enable the Utility Server, do one of the following:
   • If you want to enable the Utility Server, select Yes.
   • If you do not want to enable the Utility Server, select No.

   ! Important:
   You must either enable the Utility Server on all nodes or disable it on all nodes. You cannot enable the Utility Server on some cluster nodes and disable it on other nodes.

7. Follow the system prompts to complete the upgrade procedure.

8. Repeat the steps above on the backup node first and then on all other non-seed cluster nodes.

9. Log in to the seed node as an administrative user using an SSH connection.

10. Run the `svc aads restart` command to restart Avaya Aura® Device Services.

11. Repeat steps 9 and 10 on all other cluster nodes.

12. Verify that DRS replication is working for all nodes on System Manager.
   For more information, see Checking for DRS synchronization on page 131.

Next steps
If you enabled the Utility Server and you need to migrate data from a legacy 7.1 Utility Services machine, complete Migrating Utility Server data on page 128.

---

Rolling back the ESXi or AWS upgrade

About this task
Use this procedure to abort the upgrade procedure and roll back to the previously installed Avaya Aura® Device Services release. You can roll back to a previously installed release if that release is still present on the server.

In a cluster environment, the order for rolling back nodes is the reverse of the order used for upgrading Avaya Aura® Device Services.

You cannot use Avaya Aura® Device Services during a rollback. In a cluster environment, services are started after all nodes are rolled back.

Note:
You cannot roll back disk space allocation and system layer update procedures, which are compatible with Release 7.1.5.

Before you begin
Complete Upgrading ESXi or AWS virtual machines on page 126.

Procedure
1. Using an SSH connection, log in as an administrator to the node that you last upgraded.
2. Run the following commands to perform the rollback for this node:

```bash
cd
app rollback
```

3. Repeat the previous steps for all other nodes in the reverse order to the one you used for upgrading Avaya Aura® Device Services.

   The seed node must be the last node that you roll back.

4. Log in to the seed node as an administrator using an SSH connection.
5. Run the `svc aads start` command to start Avaya Aura® Device Services.
6. Repeat steps 4 to 5 for the backup node first and then for all other non-seed nodes.

---

**Migrating Utility Server data**

**About this task**

Use this procedure to migrate data from the legacy Avaya Aura® Utility Services to the Utility Server embedded within Avaya Aura® Device Services. This process restores a backup, which was created on the Utility Services server, into the Utility Server embedded within Avaya Aura® Device Services. Since the Utility Server uses only a subset of data from the Avaya Aura® Utility Services server, this procedure only extracts the required subset of data.

⚠️ **Important:**

- In a cluster environment, perform this procedure on all cluster nodes, starting from the seed node.
- Any active firmware packages are deactivated during this procedure.

**Procedure**

1. Create a “no firmware” backup on the legacy Avaya Aura® Utility Services machine and then store the backup file on the machine that you use to access the web administration portal.

   ⚠️ **Important:**

   Ensure that the **No firmware** backup option is used for this procedure. The legacy Avaya Aura® Utility Services servers allow you to choose whether the backup file will contain phone firmware. For disk space considerations, the Utility Server embedded within Avaya Aura® Device Services only supports backups that do not include phone firmware. You must manually upload phone firmware on the Utility Server and then unpack and activate the firmware.

2. Log in to web administration portal for the Utility Server using the following URL:

   ```
   https://<Utility_Server_address>:8543/admin.html
   ```

   Replace **Utility_Server_address** with the virtual IP address or FQDN of the Utility Server.
**Note:**

Use the user name and password of the administrative user that you created while deploying the OVA.

3. Navigate to **Miscellaneous > Utility Services Backup and Restore**
4. Click **Browse** and navigate to the backup file created in step 1.
5. Select the backup file and click **Open**.
6. Click **Upload Backup**.
7. Repeat the previous steps for all other cluster nodes.

---

### Upgrading existing test configurations

**About this task**

Upgrading Avaya Aura® Device Services may sometimes introduce new auto-configuration settings. In such a scenario, all existing auto-config test configurations must be upgraded to reflect newly introduced settings. For this, you must perform the following task.

**Procedure**

1. Log on to the Avaya Aura® Device Services server as an administrator.
2. Run the following commands:

   ```bash
   ctdo misc
   sudo ./clitool-acs.sh upgradeAutoConfigTestConfigurations
   ```

   This command automatically upgrades the existing test configurations.

---

### Running a patch to allow Avaya Equinox® for Windows to connect to the Web Deployment service

**About this task**

For software updates through Avaya Equinox® for Windows clients, you must apply a patch by following the instructions in this section. The patch opens port 8442 for the Web deployment service and sets up port 8442 to pass web deployment requests without certificate validation.

**Important:**

You must use this procedure only if you have Avaya Equinox® for Windows clients and ESG servers in your environment.
If you have only Avaya Aura® Device Services and Avaya Equinox® for Windows clients in the network, you must set the REST and OAMP fields on the Client Administration > Client Settings screen to None.

You can use the patch with the following arguments:

- **enable**: To apply the workaround to allow Avaya Equinox® for Windows to reach the Web Deployment service.
- **disable**: To revert the workaround to allow Avaya Equinox® for Windows to reach the Web Deployment service.

If the disable argument is used, the patch removes port 8442 from nginx and iptables. In this procedure, the enable argument is used to apply the workaround.

You must run this patch after every upgrade or rollback of Avaya Aura® Device Services so that the Web deployment service works for the Windows client.

**Procedure**

1. Go to `/opt/Avaya/DeviceServices/<version>/CAS/<version>/misc/`.
2. Run the following command:
   ```sh
   sudo ./webdeployment-patch.sh enable
   ```
   For example, the `sudo ./webdeployment-patch.sh enable` command displays the following messages:
   ```
   grep acs-nginx-webdeployment-8442.conf /opt/Avaya/DeviceServices/7.1.0.0.243/nginx/1.8.0-1/conf/nginx.conf
   acs-nginx-webdeployment-8442.conf will be added now
   iptables rule will be added now
   iptables: Saving firewall rules to /etc/sysconfig/iptables:
   [  OK  ]
   2017-01-24_12:17:36 Reloading Nginx ....................
   [  OK  ]
   ```

   After running the patch, you must download URL and appcast URL to use port 8442.

3. Log on to the Avaya Aura® Device Services web administration portal.
4. In the navigation pane, click **Web Deployment > Deployment**.
   The system displays the Software Update Deployment page.
5. On the Software Update Deployment page, change the Download URL port for Appcast to 8442.
   ```
   ```
6. Change the APPCAST URL port in Dynamic Configurations to 8442.
   ```
   For example, https://<AADS FQDN/IP Address>:8442/acs/resources/webdeployment.
   ```
Running a patch to allow the Avaya Aura® Web Gateway to connect to the Avaya Aura® Device Services automatic configuration service

About this task
You can perform this task only if you have the Avaya Aura® Web Gateway server set up in the Avaya Aura® Device Services environment and if the REST certificate policy is set to NONE on the Avaya Aura® Device Services web administration portal.

You must run the `dynamicconfigurations-patch.sh` script to allow the connection between the Avaya Aura® Web Gateway and Avaya Aura® Device Services automatic configuration service using the certificate policy. This patch opens the port 8440 for auto-configuration service and the Avaya Aura® Device Services provides the auto-configuration service on port 8440.

You must run this patch after every upgrade or rollback or migration of Avaya Aura® Device Services to allow the Avaya Aura® Web Gateway to reach Avaya Aura® Device Services automatic configuration service.

You can use the patch with the following arguments:

- **enable**: To open port 8440 to allow Avaya Aura® Device Services to communicate with the Avaya Aura® Web Gateway.
- **disable**: To close port 8440 from nginx and iptables.

Procedure
Run the following commands:

```
cd to misc
sudo ./dynamicconfigurations-patch.sh enable
```
Chapter 11: Troubleshooting

DRS remains in Ready to Repair state

Cause
Tomcat must restart to register the DRS URL.

Solution
Restart Tomcat.
The DRS state changes to repairing, synchronizing, and then synchronized.

DRS remains in repairing state for a long time

Cause
When Avaya Aura® Device Services logs are set to the FINEST level, large nginx logs are created during the DRS process. Writing these logs on the disk affects system performance, which causes connection timeouts.

Solution
1. Change the log level to WARN.
2. From System Manager, synchronize the node.
After the node is synchronized, you can change the log level back to FINEST.

Related links
- Setting up the log level on page 98
- Checking for DRS synchronization on page 131

DRS remains in not polling state

Condition
A DRS polling error occurs.
Cause
System Manager and Avaya Aura® Device Services are not in the same DNS or the /etc/hosts file for System Manager does not include the Avaya Aura® Device Services IP addresses and FQDN.

Solution
1. Update the System Manager /etc/hosts file to include the Avaya Aura® Device Services IP addresses and FQDNs.
2. Update the Avaya Aura® Device Services /etc/hosts file to include the System Manager IP addresses and FQDNs.
3. Run the Avaya Aura® Device Services configuration utility using the app configure command.
4. Reconfigure System Manager details again and wait until the DRS configuration process is complete.

DRS fails with constraint error

Cause
DRS replication fails with a constraint error.

Solution
1. Perform a manual repair from the System Manager web interface.
2. If the above step fails, do the following to re-register DRS:
   a. Go to the /opt/Avaya/DeviceServices/<build>/CAS/<build>/drs directory.
   b. Run the following commands in sequence:
      ```
      removeReplicationEntry.sh
drsInstall.sh
drsStart.sh
      ```

Services are not working properly after an installation or upgrade

Condition
After installing or upgrading Avaya Aura® Device Services in a cluster, services are not working properly. Log files contain an error, such as the following:

```
2017-11-10 14:34:38 ERROR datastore:191 - (ConfigurationStore.java:2166) Decryption failed for server bind credentials, setting it to original
2017-11-10 14:34:38 ERROR impl:191 - (SecurityServiceImpl.java:117) Exception occurred while decrypting data
2017-11-10 14:34:38 FINE impl:245 - (SecurityServiceImpl.java:117) Exception stack
```
Trace
javax.crypto.IllegalBlockSizeException: Input length must be multiple of 16 when decrypting with padded cipher
at com.sun.crypto.provider.CipherCore.doFinal(CipherCore.java:922)
at com.sun.crypto.provider.CipherCore.doFinal(CipherCore.java:833)
at com.sun.crypto.provider.AESCipher.engineDoFinal(AESCipher.java:446)
at javax.crypto.Cipher.doFinal(Cipher.java:2165)
at com.avaya.cas.security.impl.SecurityServiceImpl.apoKruptos(SecurityServiceImpl.java:107)
at com.avaya.cas.security.impl.SecurityServiceAdapter.apoKruptos(SecurityServiceAdapter.java:57)
at com.avaya.cas.datastore.ConfigurationStore.getServerConfigParamFromRow(ConfigurationStore.java:2164)
at com.avaya.cas.datastore.ConfigurationStore.getAllServerConfigurations(ConfigurationStore.java:2062)
at com.avaya.acs.cli.AadsCryptoToolCliApp.main(AadsCryptoToolCliApp.java:104)

Solution

1. Navigate to /opt/Avaya/DeviceServices/<version>/CAS/<version>/config and check the install.properties file.

   The files at both the nodes should have the same value for SEED_NODE.

2. If the values are different, uninstall Avaya Aura® Device Services from all nodes.

3. Run the Avaya Aura® Device Services binary installer as described in Deploying Avaya Aura® Device Services.

EASG login using craft username results in an Access Denied error

Cause
You can only paste 99 characters in PuTTY versions earlier than 0.63. Therefore, you might get an Access Denied error if you exceed the character limit.

Solution
Update PuTTY to the latest version.
ESG cannot connect to Avaya Aura® Device Services

**Condition**
ESG cannot connect to Avaya Aura® Device Services when the REST certificate policy is set to None. This occurs in deployments with Avaya Aura® Device Services and Avaya Aura® Web Gateway, if the following features are being used:

- Avaya Aura® Device Services web deployment feature for desktops.
- WebRTC call feature with Avaya Aura® Web Gateway.

**Solution**
Set the certificate validation policy in the Avaya Aura® Device Services web administration portal to Optional. Do not set the certificate validation policy to None.

Web deployment binaries for Avaya Equinox® for Windows and Avaya Equinox® for Mac must be moved to another web server or to the Avaya Aura® Device Services web server on an unchallenged web port.

⚠️ **Note:**
The Web deployment service is only accessible within the enterprise network or through VPN.

---

A new private key failed to generate

**Condition**
The Avaya Aura® Device Services configuration utility closes abruptly while configuring the SSH/RSA Public/Private keys.

**Cause**
The `/home` directory is full. Therefore, the system cannot create the `/authorized_keys` file. The log file displays a disk space warning.

**Solution**
Clean up the `/home` directory.

---

Check for Updates feature is not working

**Condition**
The Check for Updates feature on Avaya Equinox® for Windows does not work and an error is displayed.
Solution
1. On the Windows computer where the Avaya Equinox® client is installed, navigate to `C:\Windows\System32\drivers\etc\` and add the virtual FQDN of System Manager to the `hosts` file in the following format:
   `<IP Address> <virtual FQDN of System Manager>`

2. Exit the Avaya Equinox® client and ensure that the client is not running in Windows Task Manager.
3. Run the following command as an administrator:
   `ipconfig /flushdns`
4. Restart the Avaya Equinox® client.
5. If the Check for Updates feature is still not working, go to Client Settings > Support.
6. Click Reset Application.
7. Configure the Avaya Equinox® client and then log in to the client.
   You can configure the client settings using the Automatic Configuration service.

---

**Slow Avaya Aura® Device Services performance**

**Condition**
Performance is slow.

**Cause**
The network latency between all Avaya Aura® Device Services servers and their respective Session Manager servers is more than 5 ms.

**Solution**
The network latency must be less than 5 ms.

---

**Unable to access the web administration portal when the primary node Session Manager is non-operational**

**Condition**
In a cluster, if the Session Manager associated with the primary Avaya Aura® Device Services node is non-operational, the Avaya Aura® Device Services web administration portal is unavailable.

**Solution**
Use the FQDN for the other nodes to access the Avaya Aura® Device Services web administration portal when the primary node is non-operational.
PPM certificate error

Condition
If you upgrade Session Manager from a release earlier than release 6.2 FP4 to Release 7.0.1 or later before installing Avaya Aura® Device Services, the system displays a PPM certificate error while adding contacts.

Cause
The error occurs because Session Manager expects a SIP CA certificate.

Solution
1. Log in to Avaya Aura® Device Services as an administrator.
2. Go to /opt/Avaya/DeviceServices/<version>/CAS/<version>/bin.
3. Run the following command:
   ```
   sudo ./demo_certs.sh -I
   ```
   The system displays the message Certificate was added to keystore.

Repairing faulty users

About this task
The Contact Integrity Audit generates a list of faulty users, which cannot be repaired automatically. You can repair faulty users manually by de-registering or re-registering users in Avaya Aura® Device Services.

Procedure
1. Log in to Avaya Aura® Device Services as an administrator.
2. Run the cdto misc command.
3. Run the following command to get the list of faulty users:
   ```
   sudo ./clitool-acs.sh dataIntegrityAuditDiagnistics fetchFaultyUsers
   ```
4. For any faulty user you want to repair, do the following:
   a. Run the following command to de-register the user from Avaya Aura® Device Services:
      ```
      sudo ./clitool-acs.sh runUserDiagnostics -d <email address of the user>
      ```
   b. After the user is de-registered, log out and log back in to the Avaya Aura® Device Services client for the user.
5. If the faulty users are not yet repaired, investigate the user’s contact data.
**Exception in the AADS.log file**

**Condition**
When running a command in Avaya Aura® Device Services, the AADS.log file shows an exception error, such as the following:

```
ERROR 04 Dec 2017 10:00:23,846 main com.avaya.cas.management.logging -
(Log4jPropertiesConfig.java:123) IOException while reading config file /opt/Avaya/
DeviceServices/7.1.2.0.557/CAS/7.1.2.0.557/tomcat/8.0.24/lib/log4j.properties:
java.io.FileNotFoundException: /opt/Avaya/DeviceServices/7.1.2.0.557/CAS/7.1.2.0.557/
tomcat/8.0.24/lib/log4j.properties (No such file or directory)
```

**Solution**
Ignore the exception error.

**The AADS.log file contains contact integrity data**

**Condition**
The AADS.log file contains the following type of data:

```
WARN 11 Dec 2017 03:00:05,426 Audit Manager scheduling pool-3
com.avaya.acs.services.drs.core - (DataIntegrityService.java:157) Contact Integrity
audit is disabled, so no further processing will happen...
WARN 11 Dec 2017 03:00:15,430 Audit Manager scheduling pool-0
com.avaya.acs.services.drs.core - (DataIntegrityService.java:157) Contact Integrity
audit is disabled, so no further processing will happen...
WARN 11 Dec 2017 03:00:25,434 Audit Manager scheduling pool-0
com.avaya.acs.services.drs.core - (DataIntegrityService.java:157) Contact Integrity
audit is disabled, so no further processing will happen...
WARN 11 Dec 2017 03:00:35,444 Audit Manager scheduling pool-1
com.avaya.acs.services.drs.core - (DataIntegrityService.java:157) Contact Integrity
audit is disabled, so no further processing will happen...
```

**Solution**
None. If a Contact Integrity Audit is not run, then the system resources are not burdened.

**System Manager does not show Avaya Aura® Device Services alarms**

**Condition**
Even when alarms are generated on Avaya Aura® Device Services and user profiles are properly created and assigned, System Manager does not show Avaya Aura® Device Services alarms.

**Solution**
1. Log in to Avaya Aura® Device Services as the root user.
2. Go to /var/net-snmp.

3. Memorize the timestamp of the snmpd.conf file.

4. Log in to the System Manager web console and navigate to Home > Services > Inventory > Manage Serviceability Agents > Serviceability Agents.

5. From the agents list, select the Avaya Aura® Device Services node for which alarms are not displayed on System Manager.

6. On the Serviceability Agents page, select Avaya Aura® Device Services and click Manage Profiles.

7. On the next page, click Commit.

   The timestamp of the snmpd.conf file should be updated.

8. If the timestamp of the snmpd.conf file was not updated, perform the remaining steps.

   If the timestamp was updated, then you do not need to do anything else.

9. Log in to System Manager as the root user using SSH.

10. Run the locate recoverAgent.sh command to obtain the full path to the recoverAgent.sh script.

    For example:

    ```
    >locate recoverAgent.sh
    >/opt/Avaya/Mgmt/7.1.11/remoteSnmpConfig/utility/recoverAgent.sh
    ```

11. Run the following command to remove the Avaya Aura® Device Services entry from System Manager:

    ```
    sh <path_to_recoverAgent.sh> <AADS_IP_address>
    ```

    In this command, `<path_to_recoverAgent.sh>` is the full path to recoverAgent.sh and `<AADS_IP_address>` is the IP address of Avaya Aura® Device Services.

12. Log in to Avaya Aura® Device Services as the root user.

13. Run the following command:

    ```
    $SPIRIT_HOME/scripts/utils/reinitializeSnmpdConfiguration.sh
    ```

    **Note:**

    The command might fail when restarting snmpd. This is the expected behavior.

    ```
    Stopping existing snmpd service...
    Stopping snmpd (via systemctl): [ OK ]
    Restarting snmpd (via systemctl): Job for snmpd.service failed because the control process exited with error code. See "systemctl status snmpd.service" and "journalctl -xe" for details.
    [FAILED]
    Setting the reinitialized property to true
    ```

14. Run the service spiritAgent restart command.
Firmware upgrade fails for certain endpoints

**Condition**
When using the Utility Server, the firmware upgrade fails for certain endpoints, such as 9611, 9621, or 9640 phones.

**Cause**
DHCP option 242 does not have the TLSSRVRID parameter set to 0. In this case, some endpoints cannot:

- Fetch settings files and firmware from the Utility Server using HTTPS.
- Generate a certificate file that uses the Utility Server IP address as the Common Name (CN).

**Solution**
On your DHCP server, set TLSSRVRID to 0 for DHCP option 242.

The following is an example of the DHCP option 242 configuration:

```
TLSSRVR=10.103.1.39,
TLSPORT=1543, TLSSRVRID=0
```

Open LDAP replication fails

**Condition**
Open LDAP replication fails. The `/var/log/Avaya/openldap.log` file contains entries such as the following:

- Server unwilling to perform
- ldap bind failed
- syncrepl: consumer state is newer than provider

**Solution**

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:
   ```
   sudo systemctl restart slapd
   ```
3. Repeat the steps above on all remaining nodes in the cluster.
4. Review the `/var/log/Avaya/openldap.log` file and ensure that it does not contain any error messages.

   If the `/var/log/Avaya/openldap.log` file still contains error messages, do the following:
5. On all nodes in the cluster, run the following commands:
   ```
   cdto openldap
   sudo ./recover_openldap.sh
   ```
6. Enable Open LDAP replication again.
Open LDAP replication fails if Avaya Aura® Device Services uses a custom identity certificate for server interfaces

**Condition**

When you use a custom identity certificate for an Avaya Aura® Device Services service interface, Open LDAP replication might fail. The /var/log/Avaya/openldap.log file contains the TLS negotiation failure entry.

**Cause**

The custom identity certificate is applied to a single node and not to the entire cluster.

**Solution**

Re-import the custom certificate as described in Managing server interface certificates on page 27. Ensure that you select Apply For Cluster when importing the certificate.

---

**Response delay from Open LDAP**

**Condition**

Open LDAP performance is slow.

**Cause**

Avaya Aura® Device Services writes Open LDAP logs into the /var/log/Avaya/openldap.log file. Log rotation is not used for this file. If the log file size becomes too large, Open LDAP performance might decrease.

**Solution**

Avaya recommends to truncate the /var/log/Avaya/openldap.log file when the file size exceeds 30 MB.

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command to check the /var/log/Avaya/openldap.log file size:
   ```shell
   ls -lh /var/log/Avaya/openldap.log
   ```
3. If the file size is more than 30 MB, run the following command to clear the file content:
   ```shell
   sudo truncate -s 0 /var/log/Avaya/openldap.log
   ```
Allocating unused disk space to logical volumes

About this task
In rare circumstances, you might need to allocate free disk space to a specific disk volume to address unexpected disk engineering issues. Only use this procedure in these circumstances. For additional assistance, contact Avaya support.

Before you begin

- Increase the size of the disk that hosts logical volumes. For example, if a logical volume requires an additional 20.0 GiB of space and the host disk is currently 50.0 GiB, then you must change the disk size to 70.0 GiB. For more information, see Increasing the virtual disk size of ESXi virtual machines on page 144 and Increasing the virtual disk size of AWS virtual machines on page 146.

- Since the allocation of disk space to a volume cannot be undone at the operating system level, create a snapshot of the virtual machine before performing the allocation procedure. If an error occurs during the procedure, reverting to the snapshot will restore the system to the point prior to where allocations were performed. After reverting to the snapshot, you can try to perform the allocation procedure again.

Tip:
To save system resources and maintain the performance of the virtual machine, delete the snapshot after the allocation procedure is completed successfully.

On VMware ESXi, you can choose to exclude the virtual memory of the virtual machine from the snapshot. Therefore, the snapshot creation process will take less time. However, if the virtual memory is excluded from the snapshot, the state of the running application processes and other system processes is not preserved in the snapshot. Therefore, any runtime data will be lost when you revert to that snapshot. Avaya recommends that you shut down the application using the `svc aads stop` command before taking the snapshot. After you allocate disk space and delete the snapshot, start the application using the `svc aads start` command.

Procedure

1. Log in to the virtual machine as an administrative user using an SSH connection.
2. Run the following command to scan the disks on the virtual machine to detect available free space:
   ```bash
   sys volmgt --scan
   ```

   This command scans the virtual disks of the system to detect a size increase. Then the command displays the file system summary, which includes the size and amount of free storage for each virtual disk, and the size and usage of the volumes hosted on these disks.

   In the following example, 50.00 GiB of free storage is available to be allocated to the volumes on disk 1.

<table>
<thead>
<tr>
<th>Num</th>
<th>Name</th>
<th>Size</th>
<th>Free</th>
<th>Name</th>
<th>Size</th>
<th>Size</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Tip:

- You can run the `sys volmgt --h` command to get basic information on command line syntax, and the `sys volmgt --hh` command for verbose help.
- You can review summaries, such as the one above, at any time by running the `sys volmgt --summary` command. This command does not scan disks for newly available unallocated storage. Use this command if you know that disk sizes have not been increased since the last summary was displayed.

3. Run the following commands to allocate a specific amount of disk space to a volume:

```bash
sys volmgt --extend <volume> <x>[m|g|t]
```

In this command:

- `<volume>` specifies the name of the volume that is displayed when you run either the `sys volmgt --summary` or `sys volmgt --scan` command.
- `<x>` specifies amount of space. `<x>` is a decimal number.
- `m` means megabytes.
- `g` means gigabytes.
- `t` means terabytes.

For example, the following command allocates 10.5 GiB to the `/var/log` volume:

```bash
sys volmgt --extend /var/log 10.5g
```

4. Run the following command to allocate all remaining disk space to a volume on the disk:

```bash
sys volmgt --extend <volume> --remaining
```

All `--extend` operations are run as background tasks.

a. To monitor the status of the operation in progress or of the last completed operation, run one of the following commands:

```bash
sys volmgt --monitor
sys volmgt --monitor less
```

The first command uses the `tail` browser to display the results. The second command uses the `less` browser to display the results.
b. To gather all volume management logs into a .zip file in the current working directory, run the following command:

```
sys volmgt --logs
```

c. If you suspect that the reported size of a file system is not correct, check if the operation is still in progress by running the following command:

```
sys volmgt --status
```

d. If the status is reported as “Complete”, you can correct the situation by running `--extend` without an increment value:

```
sys volmgt --extend /var/log
```

This operation does not add more space to the volume that hosts the file system. Instead, it reissues the command to make full use of the volume space. The file system expansion process is part of the original `--extend` operation, which is used to increase the volume size. However, in some cases, this operation might be interrupted and require the above command to re-initiate the expansion.

---

**ESXi virtual hardware adjustments**

The following sections describe how to perform virtual hardware adjustments on ESXi virtual machines. These adjustments are external to the guest operating system of the virtual machine.

These virtual hardware adjustment procedures only apply to virtual machines hosted on VMware ESXi hosts.

⚠️ **Important:**

If you are using Appliance Virtualization Platform (AVP), avoid adjusting virtual hardware parameters because your adjustments could affect other applications hosted on the same AVP instance.

### Increasing the virtual disk size of ESXi virtual machines

**About this task**

Use this procedure to increase the size of virtual disks on existing Avaya Aura® Device Services virtual machines.

An Avaya Aura® Device Services virtual machine has three virtual disks. VMware vSphere emulates the physical environment very closely. Therefore, virtual disks of a virtual machine can be referred to as “hard disks”.

<table>
<thead>
<tr>
<th>Disk number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard disk 1</td>
<td>Operating system and application software.</td>
</tr>
<tr>
<td>Hard disk 2</td>
<td>Application logs.</td>
</tr>
<tr>
<td>Hard disk 3</td>
<td>Application data.</td>
</tr>
</tbody>
</table>
**Note:**
You cannot reduce the disk size.

**Procedure**
1. Log in to the virtual machine as an administrative user using an SSH connection.
2. Run the following command to perform a graceful shutdown of the virtual machine operating system and to power off the virtual machine:
   ```
   sudo shutdown -hP now
   ```
3. Using the vSphere client, log in to either the vCenter server or ESXi host.
4. Delete all virtual machine snapshots.
   **Note:**
   You cannot modify the size of virtual disks when snapshots exist on the system.
5. In the vSphere client inventory, right-click the required virtual machine and then select **Edit Settings**.
6. Navigate to the Virtual Hardware tab.
7. Select the desired unit size, such as GB, TB, or MB, and enter the new value for the disk size.
   **Important:**
   Perform this step with caution because updating the disk size cannot be undone. Make sure you use the desired units and the disk size value. Otherwise, you might need to delete the virtual machine and deploy a new OVA.
8. Click **OK**.
9. Repeat steps 5 to 8 if you need to increase the disk size of any other virtual disks.

**Next steps**
Distribute the allocated free space between the logical volumes as described in Allocating unused disk space to logical volumes on page 142.

**Adjusting the CPU and memory resources of the Avaya Aura® Device Services virtual machine**

**About this task**
Use this procedure only in a VMware virtualized environment.

**Before you begin**
Install VMware with an Enterprise Plus license.

**Procedure**
1. Shut down the Avaya Aura® Device Services virtual machine.
2. In the vSphere client inventory, right-click the Avaya Aura® Device Services virtual machine and select **Edit Settings**.

3. In the Virtual Machine Properties window, in the Hardware tab, click **Memory** or **CPUs**.

4. Do one of the following:
   - Change the memory configuration.
   - Change the CPU settings.

5. Click **OK** to exit the window.

6. Restart the Avaya Aura® Device Services virtual machine.

---

### Increasing the virtual disk size of AWS virtual machines

**About this task**

Use this procedure to increase the size of on an existing Avaya Aura® Device Services virtual machine.

The following table shows the three virtual disks and the block devices of these disks, which are used by Avaya Aura® Device Services virtual machines on AWS.

<table>
<thead>
<tr>
<th>Disk number</th>
<th>Block device</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk 1</td>
<td>/dev/sdal</td>
<td>Stores operating system and application software.</td>
</tr>
<tr>
<td>Disk 2</td>
<td>/dev/xvdb</td>
<td>Stores application logs.</td>
</tr>
<tr>
<td>Disk 3</td>
<td>/dev/xvdc</td>
<td>Stores application data.</td>
</tr>
</tbody>
</table>

**Note:**

You cannot reduce the disk size.

**Procedure**

1. On the AWS console, navigate to Services > Compute, and then click **EC2**.
2. On the EC2 Management Console page, click **Instances**.
3. Select the instance to which you want to add storage.
   - The system displays instance details.
4. Click the **Description** tab.
5. In the **Block devices** field, select a disk for which you want to increase the size.
   - The options are:
     - disk1
     - disk2
     - disk3
**Note:**
A system restart is required when you change the size of disk1. If you do not modify disk1, a system restart is not required.

6. In the **EBS ID** field, click the ID.

   The system displays the Volumes page with only the selected device.

7. To update the storage on the EBS disk volume, click **Actions > Modify Volume**.

8. In the Modify Volume window, in the **Size** field, enter the required disk size.

9. Click **Modify**.

10. In the Confirmation window, click **Yes**.

11. In the Status window, click **Close**.

12. If you updated disk1, do the following to restart the system for the changes to take effect:
   a. Log in to the virtual machine as an administrative user using an SSH connection.
   b. Run the `sudo reboot` command.

      If Avaya Aura® Device Services is running when you run this command, then Avaya Aura® Device Services will be gracefully shut down.

**Note:**
The process of increasing the disk size might take some time to complete. Monitor the size of the virtual disks and only proceed with any other disk-related activities after the size changes take effect.

**Next steps**
Distribute the allocated free space between the logical volumes as described in [Allocating unused disk space to logical volumes](#) on page 142.

---

**Cannot reinstall a non-seed node due to Cassandra startup error**

**Condition**
When reinstalling a non-seed node, Avaya Aura® Device Services becomes unresponsive while trying to start the Cassandra database.

**Cause**
If the non-seed node was not uninstalled from the cluster properly, then it remains as a registered cluster node in the Cassandra database.
Solution

1. On the non-seed node, run the following command to uninstall the node:

   `sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/uninstaller/uninstallAADS.sh`

2. On the seed node, run the following command to restart services:

   `svc aads restart`

3. Reinstall the non-seed node.
# Chapter 12: Resources

## Documentation

The following table lists related documentation. All Avaya documentation is available at [https://support.avaya.com](https://support.avaya.com). Many documents are also available at [https://documentation.avaya.com/](https://documentation.avaya.com/).

<table>
<thead>
<tr>
<th>Title</th>
<th>Use this document to:</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Implementing</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>Deploying Avaya Aura® Device Services</em></td>
<td>Deploy Avaya Aura® Device Services.</td>
<td>Sales engineers, solution architects, implementation engineers, support personnel</td>
</tr>
<tr>
<td><em>Deploying Avaya Aura® Session Manager</em></td>
<td>Deploy the Session Manager OVA.</td>
<td>Sales engineers, solution architects, implementation engineers, support personnel</td>
</tr>
<tr>
<td><strong>Administering</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>Administering Avaya Aura® Device Services</em></td>
<td>Administer Avaya Aura® Device Services.</td>
<td>System administrators, support personnel</td>
</tr>
<tr>
<td><em>Administering Avaya Aura® Session Manager</em></td>
<td>Administer the Session Manager interface.</td>
<td>System administrators, support personnel</td>
</tr>
</tbody>
</table>
| *Planning for and Administering Avaya Equinox® for Android, iOS, Mac, and Windows* | Perform system planning and configuration for:  
  - Avaya Equinox® for Android  
  - Avaya Equinox® for iOS  
  - Avaya Equinox® for Mac  
  - Avaya Equinox® for Windows | System administrators, support personnel |
| **Using** | | |
| *Using Avaya Device Enrollment Services to Manage Endpoints* | Use Device Enrollment Services to manage endpoints or devices. | Non-Avaya users, such as service providers and resellers |

October 2019  
Administering Avaya Aura® Device Services  
Comments on this document? infodev@avaya.com
Finding documents on the Avaya Support website

Procedure

2. At the top of the screen, type your username and password and click Login.
3. Click Support by Product > Documents.
4. In Enter your Product Here, type the product name and then select the product from the list.
5. In Choose Release, select an appropriate release number.
6. In the Content Type filter, click a document type, or click Select All to see a list of all available documents.
   For example, for user guides, click User Guides in the Content Type filter. The list displays the documents only from the selected category.
7. Click Enter.

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at https://documentation.avaya.com.

⚠️ Important:

For documents that are not available on the Avaya Documentation Portal, click Support on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Portal, you can:

• Search for content in one of the following ways:
  - Type a keyword in the Search field.
- Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.

- Select a product or solution and then select the appropriate document from the list.

* Find a document from the **Publications** menu.

* Publish a PDF of the current section in a document, the section and its subsections, or the entire document.

* Add content to your collection by using **My Docs** (🌟).

Navigate to the **My Content > My Docs** menu, and do any of the following:
- Create, rename, and delete a collection.
- Add content from various documents to a collection.
- Save a PDF of selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive content that others have shared with you.

* Add yourself as a watcher by using the **Watch** icon (👁️).

Navigate to the **My Content > Watch list** menu, and do the following:
- Set how frequently you want to be notified, starting from every day to every 60 days.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.

* Share a section on social media platforms, such as Facebook, LinkedIn, Twitter, and Google +.

* Send feedback on a section and rate the content.

**Note:**

Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

---

**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 [https://support.avaya.com/](https://support.avaya.com/) and do one of the following:
  - 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](http://www.youtube.com/AvayaMentor) and do one of the following:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

**Note:**
Videos are not available for all products.

Support

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

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.
Use the Avaya InSite Knowledge Base for any potential solutions to problems.

2. Log on to the Avaya website with a valid Avaya user ID and password. The system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press **Enter**.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.
Appendix A: Additional administration tools

You can use the following tools for Avaya Aura® Device Services administration:

• The JConsole java tool

   JConsole uses the extensive instrumentation of the Java Virtual Machine (Java VM) to provide information about the performance and resource consumption of applications running on the Java platform.

   You can use jconsole to monitor the following components:
   - Tomcat
   - Serviceability Agent (also known as spiritAgent)

   For more information about using the jconsole utility, see the Oracle documentation.

 Important:

   JConsole is a graphical tool and can be run locally from an Avaya Aura® Device Services node that has a graphical desktop environment installed.

• Avaya Aura® Device Services tools such as clitool-acs, and collectLogs.

   - clitool-acs
     A tool that has multiple usage possibilities. The parameters specified in the command determine the usage of the clitool-acs utility.

   - collectLogs
     Enables you to collect and download the logs from an Avaya Aura® Device Services node.

   - statusAADS
     A tool that displays the status of the Avaya Aura® Device Services server and of the related services.

     The statusAADS.sh script is located in the /opt/Avaya/DeviceServices/<version>/CAS/<version>/bin directory.

• Linux tools such as ping, nslookup, ip, ethtool, wget, and curl

   - ping
Sends an ICMP ECHO_REQUEST to network hosts.
- nslookup
  Queries the internet servers interactively.
- ip
  Displays and manages routing devices, policy routing and tunnels.
  You can use this command to identify nodes that have a virtual IP address.
- ethtool
  Queries and manages network driver and hardware settings.
  You can use this command to confirm that the physical network adaptor is enabled and available.
- wget
  Downloads files from the Web.
  You can use this tool to perform resource discovery for a user.
- curl
  Transfers a URL.

**clitool-acs**

The clitool-acs utility provides multiple usage possibilities, depending on which parameters the utility receives in the command line.

**Usage example**

Run the clitool-acs.sh utility with the appropriate parameters. To view the command options, run the clitool-acs.sh utility without any parameters.

**Note:**

The clitool.sh utility does not create report directories automatically. You must create a report directory and set the read, write, and execute permissions to this directory before running the clitool.sh utility using the following commands:

```
mkdir <report_directory>
sudo chmod 777 <report_directory>
```

For example:

```
[admin@srvr-dev-114 ~]$ cdto misc
[admin@srvr-dev-114 misc]$ sudo ./clitool-acs.sh
Usage:
clitool-acs.sh listClusterNodes
clitool-acs.sh applicationInterface <start|stop>
```
clitool-acs.sh removeClusterNode <serverUUID> [force]
cloitool-acs.sh clusterVirtualIp [virtual IP address] master|backup|clear [node IP address]
cloitool-acs.sh systemManagerUPM [recommended System Manager UPM user and password]
cloitool-acs.sh pushKeytab
clitool-acs.sh registerClusterNode <serverUUID> <IP address> [force]
cloitool-acs.sh longpollTimeout [longpoll timeout duration]
cloitool-acs.sh ldapConfiguration [ldap properties filename] <ldap user's password> --current
clitool-acs.sh corsConfiguration [cors properties filename]
cloitool-acs.sh certWarningPeriod [number of days]
cloitool-acs.sh notificationFrontend [http|websocket|schemeHTTP|schemeWebsocket|host|port] <schemeWSS> <schemeHTTP> <host IP or name> <port>
cloitool-acs.sh checkVersions
cloitool-acs.sh clientCertificateVerificationConfig [service_name] off|optional|on
clitool-acs.sh restFrontend [scheme] <host> <port>
cloitool-acs.sh licenseServerUrl <ip/fqdn> <port>
cloitool-acs.sh drsSyncDuration [recommended DRS sync duration timeout]
cloitool-acs.sh microsoftExchangeServer [recommended Microsoft Exchange Server Details]

**collectLogs**

The **collectLogs** utility copies the logs from an Avaya Aura® Device Services node to a file or to a directory specified as parameters in the command.

**Usage example**

- `$ app collectlogs collect -n 2`: creates an archive with a log history to a count of two.
  - `$ app collectlogs collect -d /tmp/ -n 2 -nt`: copies the log files to the /tmp directory with a log history to a count of two. The -nt option indicates no tar so that the log files are collected in the specific directory but not combined in to a single archive.
  - `$ app collectlogs -d /tmp/ -name <archive_name>`: creates an archive of the log files that prefixes <archive_name> to the filename in the /tmp directory with each of the log files to the maximum log history depth of twenty.

**statusAADS utility**

The **statusAADS.sh** utility displays the status of the Avaya Aura® Device Services server and of the related services.

**Usage example**

Run the **statusAADS.sh** script from `/opt/Avaya/DeviceServices/<version>/CAS/<version>/bin`. 

Comments on this document? infodev@avaya.com
Checking Avaya Aura® Device Services status

Procedure

1. Log in to the Avaya Aura® Device Services CLI.
2. Type `svc aads status`.

   The system displays the current status of Avaya Aura® Device Services

Shutting down Avaya Aura® Device Services gracefully

Procedure

1. Log in to the Avaya Aura® Device Services CLI.
2. Run the following command:

   `svc aads stop`

System layer commands

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

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

Execute system layer commands.

```
-h, --help
```
Verbose help information

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

\begin{verbatim}[admin@server-dev ~]$ sys -hh
\end{verbatim}

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

\begin{verbatim}

\textbf{secconfig} \\
\hspace{1em} Manages security-related settings.

\textbf{versions} \\
\hspace{1em} Queries the version information of various elements of the system layer.

\textbf{volmgt} \\
\hspace{1em} Queries the sizes of existing disk volumes and extends their sizes.

\textbf{smcvmgt} \\
\hspace{1em} Manages the enablement status of Linux kernel patches for the Spectre and Meltdown vulnerabilities.
\end{verbatim}

\begin{verbatim}[admin@server-dev ~]$\end{verbatim}

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

\section*{sys secconfig command}

\textbf{sys secconfig} provides access to the \texttt{secconfig} command, which existed in previous releases. The following is an example of this command:

\begin{verbatim}[admin@server4950aads ~]$ sys secconfig --hhelp
\end{verbatim}

This script is used to manage run-time security settings on this appliance. The following command-line arguments are available:
---help, -h
  Prints terse help (command line syntax).

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

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

---sys versions command

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

```
[admin@server4889aads ~]$ sys versions
Appliance type : AADS
System layer version : 3.4.1.0.3
Partitioning version : 2.0
Original OVA deploy : aads-7.1.5.0.117
```

---sys volmgt command

**Syntax help: sys volmgt --help**

The **sys volmgt** command is used to query and extend disk volumes on the system. The
following provides the command line syntax for this command:

```
[admin@server4889aads ~]$ sys volmgt --help
Syntax:
  --help,                  -h
  --hhelp,                 -hh
  --version,               -v
  --status,                -st
  --summary,               -s
  --monitor  [tail|less],  -m [tail|less]
  --logs,                  -l
  --scan
  --extend <volume> [ <n>m | <n>g | <n>t --remaining ]
  --extend --all
  --reset
```

[admin@server4889aads ~]$
Verbose help: sys volmgt --hhelp

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

```
[admin@server4889aads ~]$ sys volmgt --hhelp
```

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

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

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

The above example will do two things:

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

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

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

```
sys volmgt --extend /var/log/Avaya
```

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

```
sys volmgt --extend --all
```

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

Note the following general points regarding this script:

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

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

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

```
sys volmgt --status
```

- Logical volumes on the system are referenced using their Linux file system mount points, such as /var/log/Avaya and /media/data, with the exception of the volume containing Linux swap, which has no mount point. The Linux swap volume is referenced using "swap".
- Sizes are specified in base 2 units rather than base 10 (SI) units. For example, 1g = 1 GiB = 1024 x 1024 x 1024 bytes.

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

- Due to file system overhead allocation by the Linux kernel, the size of a file system will never exactly match the size as reported by the LVM volume that contains that file system. To be certain that a file system is fully extended to the size of the volume that contains it, inspect the log file after issuing the extend operation as follows:

  sys volmgt --monitor less

To perform such a check across all volumes:

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

The following arguments are supported by this script:

--help, -h
Terse help.

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

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

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

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

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

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

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

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

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

```
--extend <volume> [ <n>m | <n>g | <n>t --remaining ]--extend --all
```

The first form of the command operates on a single volume. If a size is specified, then the LVM volume is extended by that size (step 1), and the file system it contains is extended to use the new space made available in that volume (step 2). If a size is not specified, then the file system contained in that volume is extended (i.e., step 2 only).

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

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

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

The smallest increment that can be specified is 100 MiB.

Example invocations:

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

```
--reset
```

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

```
[admin@server4889aads ~]$ sys volmgt --summary
```

### Partitioning examples: sys volmgt --summary

Avaya Aura® Device Services supports partitioning versions 1.0 and 2.0.

The following example shows a summary of the information provided by this command for a version 1.0 partitioned system:

```
[admin@server4889aads ~]$ sys volmgt --summary
```

```
Disk and Volume Summary

+------------+-------------------+-----------------------------------------------+
| Num | Name | Size | Free | LVM | File System | Size | Size | Usage | 
+------------+-------------------+-----------------------------------------------+
| 2 | sdb | 25.00 | 0.00 | /home | 4.00 | 3.94 | 1.49 | 
```

Comments on this document? infodev@avaya.com
The following example shows a summary of the information provided by this command for a version 2.0 partitioned system:

```
[admin@server4950aads ~]$ sys volmgt -s
Disk and Volume Summary

<table>
<thead>
<tr>
<th>Num</th>
<th>Name</th>
<th>Size</th>
<th>Free</th>
<th>Name</th>
<th>LVM</th>
<th>File System</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>sda</td>
<td>124.51</td>
<td>50.10</td>
<td>/</td>
<td>17.30</td>
<td>17.29</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/home</td>
<td>4.00</td>
<td>3.99</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/opt/Avaya</td>
<td>14.70</td>
<td>14.69</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/tmp</td>
<td>14.90</td>
<td>14.89</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var</td>
<td>8.50</td>
<td>8.49</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/log</td>
<td>5.00</td>
<td>4.99</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>/var/log/audit</td>
<td>6.00</td>
<td>5.99</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>swap</td>
<td>4.00</td>
<td>n/a</td>
</tr>
<tr>
<td>2</td>
<td>sdb</td>
<td>70.00</td>
<td>0.00</td>
<td>/var/log/Avaya</td>
<td>70.00</td>
<td>69.98</td>
</tr>
<tr>
<td>3</td>
<td>sdc</td>
<td>40.00</td>
<td>0.00</td>
<td>/media/data</td>
<td>40.00</td>
<td>39.99</td>
</tr>
<tr>
<td>4</td>
<td>sdd</td>
<td>10.00</td>
<td>0.00</td>
<td>/media/cassandra</td>
<td>10.00</td>
<td>9.99</td>
</tr>
</tbody>
</table>
```

**sys smcvmgmt command**

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

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

**Note:**

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

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

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

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

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

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

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

Syntax help: `sys smcvemgt --help`

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

Version 1.2

Syntax:
--help,  -h
--hhelp, -hh
--query, -q
--set,  -s enabled
--set,  -s disabled
--set,  -s [ v2=<v2-mode> ] [ v3=<v3-mode> ]
    (v2-mode: disabled | default | kernel | user | both | user+retp)
    (v3-mode: disabled | enabled)
--history
```

Verbose help: `sys smcvemgt --hhelp`

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

Version 1.2

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

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

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

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

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

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

[https://access.redhat.com/articles/3311301](https://access.redhat.com/articles/3311301)

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

[https://access.redhat.com/security/vulnerabilities/speculativeexecution](https://access.redhat.com/security/vulnerabilities/speculativeexecution)
Syntax:

```
--help,  -h
 Provide terse help.

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

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

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

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

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

v2-mode:

disabled
 Variant #2/Spectre is disabled.

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

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

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

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

user+retp
 Use "retpoline,ibrs_user".

v3-mode:

disabled
 Variant #3/Meltdown is disabled.

enabled
 Variant #3/Meltdown is enabled.

The following two commands are equivalent:

sys smcvmgmt enabled
```
sys smcvemgt v2=default v3=enabled

The following two commands are equivalent:

sys smcvemgt disabled
sys smcvemgt v2=disabled v3=disabled

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

sys smcvemgt usage examples

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

sys smcvemgt --query

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

sys smcvemgt --set enabled

Commands for enabling patches with specific settings
- The following command enables patches for Variant #2/Spectre and Variant #3/Meltdown, where Variant #2/Spectre is set to kernel space only.
  sys smcvemgt --set v2=kernel v3=enabled
- The following command enables patches for Variant #2/Spectre, which are configured for user space with “Retpoline”, or “return trampoline”. Variant #3/Meltdown retains its current settings.
  sys smcvemgt --set v2=user+retp

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

sys smcvemgt --set disabled

Command for disabling patches for a specific vulnerability
The following command disables patches for Variant #3/Meltdown. Variant #2/Spectre retains its current settings.

sys smcvemgt --set v3=disabled

Aliases

Aliases provide an alternate and convenient way to run commonly used commands without specifying long path names. The arguments available for the original commands apply for the command aliases as well.
### Aliases

<table>
<thead>
<tr>
<th>Alias</th>
<th>Description</th>
</tr>
</thead>
</table>
| app   | Provides commands for application-specific tasks such as backup, restore, and view status. If you type app without arguments, the system displays the available subcommands.  
For example, the following commands give the same results:  
- `sudo /opt/Avaya/DeviceServices/version/CAS/bin/backupAADS.sh`  
- `app backup` | |
| svc   | Provides commands for managing services, such as starting, stopping, and viewing status. If you type svc without arguments, the system displays the available subcommands.  
For example, to start Avaya Aura® Device Services services, run the `svc aads start` command. | |
| cdto  | Provides an easy way to navigate through directories of the installed application. If you type cdto without arguments, the system displays the available subcommands.  
For example, the following commands give the same results:  
- `cd /opt/Avaya/DevicesServices/version/CAS/version`  
- `cdto cas` | |

### app commands

The following table displays the available **app** commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>app install</td>
<td>Runs the staged application installer.</td>
</tr>
<tr>
<td>app status</td>
<td>Displays Avaya Aura® Device Services status information.</td>
</tr>
<tr>
<td>app configure</td>
<td>Runs the configuration utility.</td>
</tr>
<tr>
<td>app listnodes</td>
<td>Displays information about the server nodes.</td>
</tr>
<tr>
<td>app collectlogs</td>
<td>Collects logs from an Avaya Aura® Device Services node.</td>
</tr>
<tr>
<td>app backup</td>
<td>Creates backup files on all Avaya Aura® Device Services nodes.</td>
</tr>
<tr>
<td>app restore</td>
<td>Restores Avaya Aura® Device Services data from a backup file on the current node.</td>
</tr>
<tr>
<td>app upgrade</td>
<td>Upgrades Avaya Aura® Device Services on the current node.</td>
</tr>
<tr>
<td>app rollback</td>
<td>Aborts the upgrade procedure and rolls back to the previously installed Avaya Aura® Device Services release.</td>
</tr>
<tr>
<td>app removeinactive</td>
<td>Removes the inactive Avaya Aura® Device Services version.</td>
</tr>
<tr>
<td>app uninstall</td>
<td>Uninstalls Avaya Aura® Device Services.</td>
</tr>
</tbody>
</table>
To receive information about a particular command, run it with the `-h` argument. For example: `app backup -h`

⚠️ **Important:**

If Avaya Aura® Device Services is not installed, then only the `app install` command is available. Other commands become available after Avaya Aura® Device Services is installed.

---

cdto commands

The following table lists the available `cdto` commands and directories that become the current directory after running the corresponding command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Navigation target</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdto base</td>
<td><code>/opt/Avaya</code></td>
</tr>
<tr>
<td>cdto root</td>
<td><code>/opt/Avaya/DeviceServices</code></td>
</tr>
<tr>
<td>cdto active</td>
<td><code>/opt/Avaya/DeviceServices/&lt;version&gt;</code></td>
</tr>
<tr>
<td>cdto cas</td>
<td><code>/opt/Avaya/DeviceServices/&lt;version&gt;/CAS/&lt;version&gt;</code></td>
</tr>
<tr>
<td>cdto misc</td>
<td><code>/opt/Avaya/DeviceServices/&lt;version&gt;/CAS/&lt;version&gt;/misc</code></td>
</tr>
<tr>
<td>cdto bin</td>
<td><code>/opt/Avaya/DeviceServices/&lt;version&gt;/CAS/&lt;version&gt;/bin</code></td>
</tr>
<tr>
<td>cdto config</td>
<td><code>/opt/Avaya/DeviceServices/&lt;version&gt;/CAS/&lt;version&gt;/config</code></td>
</tr>
<tr>
<td>cdto logs</td>
<td><code>/opt/Avaya/DeviceServices/&lt;version&gt;/CAS/&lt;version&gt;/logs</code></td>
</tr>
<tr>
<td>cdto ilogs</td>
<td><code>/opt/Avaya/DeviceServices/.AADSInstallLogs</code></td>
</tr>
<tr>
<td>cdto tlogs</td>
<td><code>/opt/Avaya/DeviceServices/&lt;version&gt;/tomcat/&lt;Tomcat version&gt;/logs</code></td>
</tr>
<tr>
<td>cdto openldap</td>
<td><code>/opt/Avaya/DeviceServices/&lt;version&gt;/CAS/&lt;version&gt;/openldap</code></td>
</tr>
</tbody>
</table>
Glossary

Cassandra
Third party NoSQL database, which is used by Avaya Multimedia Messaging to store messaging data and configuration information. For more information, see https://cassandra.apache.org/.

Domain Name System (DNS)
A system that maps and converts domain and host names to IP addresses.

Endpoints
Refers to Avaya Vantage™ and supported hard phones, including the J100 and 9600 series phones. Avaya Equinox® clients are referenced separately in this document.

Fully Qualified Domain Name (FQDN)
A domain name that specifies the exact location of the domain in the tree hierarchy of the Domain Name System (DNS).

Network Time Protocol (NTP)
A protocol used to synchronize the real-time clock in a computer.

Secure Shell (SSH)
Secure Shell (SSH) is a group of standards and an associated network protocol that the system can use to establish a secure channel between a local and a remote computer. SSH uses public-key cryptography to mutually authenticate a user and a remote computer. SSH uses encryption and message authentication codes to protect the confidentiality and integrity of the data that is exchanged between the two computers.

Simple Network Management Protocol (SNMP)
A protocol for managing devices on IP networks.

SSL (Secure Sockets Layer) Protocol
The SSL protocol is the leading security protocol on the Internet. It runs above the TCP/IP protocol and below higher-level protocols such as HTTP or IMAP. SSL uses TCP/IP on behalf of the higher-level protocols and, in the process, allows an SSL-enabled server to authenticate itself to an SSL-enabled client.

TCP
Transmission Control Protocol.

TLS
Transport Layer Security
Glossary

**UDP**  
User Datagram Protocol. This is a communication method, similar to TCP.
Index

A

AADS
  AADS overview ......................................................... 14
  overview .............................................................. 14
access denied error .................................................. 134
activate
  firmware package ............................................... 69
  adding
    LDAP server ..................................................... 34
    trusted host ..................................................... 47
additional base context DN ........................................ 42
adjusting virtual hardware parameters .................... 144
Admin Interface
  enabling Cross-Origin resource sharing ................... 52
administration tools
  cltool-acs ......................................................... 155
  collectLogs ....................................................... 156
alarms
  descriptions ....................................................... 100
  System Manager does not show AADS alarms ........... 138
aliases ................................................................. 166
allocate
  disk space to logical volumes ................................ 142
appcast item
  field descriptions ................................................ 55
app command ......................................................... 167
architecture diagram
  Avaya Aura Device Services ................................... 15
  automatic configuration service ............................... 131
Avaya Aura Device Services ................................... 20
  administration tools ............................................ 154
  topology .......................................................... 15
Avaya Breeze
  importing identity certificate to AADS .................... 31
Avaya Equinox
  configuring contact search options ....................... 21
  uploading installation files on web deployment service 53
Avaya support website support ................................ 152
AVP
  adjusting parameters .......................................... 144
  completing upgrade .......................................... 122
  deploying new virtual machines ......................... 121
  rolling back upgrade ....................................... 123
  upgrading virtual machines ................................ 120
AVP upgrade
  preparing for upgrade ........................................ 118
AWS ................................................................. 96

B

back up (continued)
  AADS deployed on ESXi or AWS ............................ 125
  phone model to group ID mapping ......................... 66
  phone settings .................................................. 64
  Utility Server ................................................... 65
backup and restore .............................................. 107
bulk import
  field descriptions ............................................. 86
  overview ......................................................... 83
  supported special characters ............................... 85
  user data to Open LDAP ....................................... 50
bulk upload
  CSV file structure ............................................. 49

C

Cassandra
  does not start when reinstalling node .................... 147
cdto command ....................................................... 168
Certificate Policy .................................................. 135
certificates
  importing Avaya Breeze authorization certificate ........ 31
  certificate signing request ................................. 25
certificate parameter description
  CPU ..................................................................... 145
  memory ............................................................ 145
certifying
  DRS synchronization ........................................... 131
  status .............................................................. 157
client certificate policy .......................................... 28
  client downloading statistics ............................... 57
clients
  uploading Avaya Equinox installation files .............. 53
cluster
  restoring .......................................................... 109
  cluster nodes
    field descriptions ........................................... 97
  collection
    delete ........................................................... 150
    edit name ...................................................... 150
    generating PDF .............................................. 150
    sharing content ............................................ 150
commands
  system layer ..................................................... 157
  command values
    Windows Domain Controller ............................... 93
    components .................................................... 16
    Avaya Aura Device Services .............................. 16
configuration
  active directory ............................................... 92
  automatic configuration flow ............................... 15
  field descriptions ............................................ 76
| Index |
|-----------------|--------|
| **configuration (continued)** |  |
| iWA | 91, 92 |
| setting | 77 |
| Windows Domain Controller | 92 |
| configuring |  |
| client certificate policy for REST | 29 |
| contact search | 21 |
| software update deployment | 53 |
| windows authentication | 43 |
| contact integrity logs disabled | 138 |
| content |  |
| publishing PDF output | 150 |
| searching | 150 |
| sharing | 150 |
| watching for updates | 150 |
| CORS configuration |  |
| cross-origin resource sharing | 51 |
| CPU and Memory | 145 |
| creating |  |
| new configuration | 75, 87 |
| CSR |  |
| connecting AADS to Avaya Aura Web Gateway | 24 |
| create | 24 |
| custom files |  |
| accessing | 64 |
| uploading on Utility Server | 63 |
| viewing | 63 |
| **D** |  |
| daily reports | 155 |
| deactivate |  |
| firmware package | 71 |
| Defaults |  |
| field descriptions | 87 |
| deleting |  |
| appcast item | 56 |
| deploy |  |
| new AVP virtual machine | 121 |
| descriptions |  |
| certificate assignment | 27 |
| DHCP server | 60 |
| diagram |  |
| automatic configuration flow | 15 |
| disk size |  |
| increasing ESXi VM disk size | 144 |
| documentation portal | 150 |
| finding content | 150 |
| navigation | 150 |
| document changes | 9 |
| downloading |  |
| Avaya Equinox clients from web deployment service | 53 |
| downloading system layer | 114 |
| DRS |  |
| fails with constraint error | 133 |
| not polling | 132 |
| ready to repair | 132 |
| **DRS (continued)** |  |
| repairing state | 132 |
| dynamic configuration |  |
| AADS-specific parameters | 78 |
| creating new configuration | 75 |
| dynamic configuration service | 31 |
| overview | 72 |
| dynamic configuration settings |  |
| assigning group identifiers to phone models | 75 |
| implementation | 74 |
| importing | 82 |
| **E** |  |
| EASG |  |
| removing | 106 |
| editing |  |
| appcast item | 56 |
| enabling |  |
| Cross-Origin resource sharing for Admin Interface | 52 |
| Cross-Origin resource sharing for Service Interface | 51 |
| enhanced access security gateway after OVA deployment | 105 |
| Split Horizon DNS mapping | 89 |
| endpoints |  |
| firmware upgrade is not working | 140 |
| enterprise directory attribute mappings |  |
| modifying | 43 |
| Enterprise LDAP Server Configuration |  |
| field descriptions | 35 |
| ESG | 135 |
| ESXi |  |
| increasing virtual disk size | 144 |
| external load balancer |  |
| enabling | 21 |
| extracting system layer | 114 |
| **F** |  |
| field descriptions |  |
| application properties | 20 |
| finding content on documentation portal | 150 |
| firmware |  |
| updating path to 46xxsetting.txt file in upgrade file | 70 |
| upgrade is not working | 140 |
| firmware package |  |
| activating | 69 |
| firmware package | 67 |
| deactivating | 71 |
| removing | 71 |
| statuses | 67 |
| unpacking | 68 |
| firmware packages |  |
| checking free space on Utility Server | 61 |
Index

phone model to group ID mapping               ...66
backup                                      ...66
restore                                      ...66
phone settings
backing up                                   ...64
picture configuration                        ...57
port                                         ...
Web Deployment                                ...53
PPM certificate error                        ...137
prerequisites
IWA                                          ...91
primary node                                 ...136
processing CA signing requests               ...26
provenance priority                         ...45
published settings                           ...81
publishing
configuration settings                      ...80

R
reinstall
cannot reinstall non-seed node              ...147
related documentation                      ...149
remove
firmware package from the Utility Server    ...71
removing
EASG                                         ...106
repairing faulty users                       ...137
restore
phone model to group ID mapping             ...66
Utility Server data                         ...66
restoring
cluster                                       ...109
standalone system                            ...108
retrieving
configuration settings                      ...82
roll back
ESXi or AWS upgrade                        ...127
roll back AVP upgrade                       ...123

searching for contacts in Avaya Equinox     ...21
configuring                                 ...21
searching for content                       ...150
secure LDAP certificate                     ...
importing using the web administration portal ...28
Server Address and Credentials
field descriptions                           ...35
Service Interface
    enabling Cross-Origin resource sharing   ...51
settings
user, group, global, platform, and exception ...77
settings file
AADS-specific parameters                    ...78
setting up
DHCP server for Utility Server              ...60
IWA                                          ...94
Serviceability Agents                       ...104
user synchronization                        ...45
sharing content                             ...150
shutting down
Avaya Aura Device Services                  ...157
special characters
    for dynamic configuration settings      ...85
    for ldap attributes                      ...47
Split Horizon DNS mapping
overview                                      ...88
Split Horizon DNS Mapping
    field descriptions                      ...90
staged system layer                          ...115
staging system layer                         ...114
standalone system                            ...
    restoring                               ...108
start                                         ...20
starting Utility Server                     ...61
status
    checking                                 ...157
    statusAADS
        usage                                ...156
    stopping Utility Server                ...61
support                                       ...152
sys                                           ...157
sys seconfig                                 ...158
sys smcvemgt                                 ...163
    examples                                ...166
system layer
    commands                                 ...157
    seconfig                                 ...158
    smcvemgt                                 ...163, 166
    versions                                 ...159
    volmgt                                   ...159
system layer (OS)                            ...113
system update                                ...113
sys versions                                 ...159
sys volmgt                                   ...159

T
testing
configuration settings                      ...79
TLS negotiation failure                      ...141
troubleshooting                              ...133, 138

U
unpack
firmware package                             ...68
update
    system layer (OS)                       ...113
<table>
<thead>
<tr>
<th>Upgrade</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>AADS deployed on ESXi or AWG</td>
<td>125</td>
</tr>
<tr>
<td>AADS deployed on AVP</td>
<td>116</td>
</tr>
<tr>
<td>AVP virtual machines</td>
<td>120</td>
</tr>
<tr>
<td>ESXi or AWS virtual machines</td>
<td>126</td>
</tr>
<tr>
<td>Preparing for AVP upgrade</td>
<td>118</td>
</tr>
<tr>
<td>Rolling back AVP upgrade</td>
<td>123</td>
</tr>
<tr>
<td>Rolling back ESXi or AWS upgrade</td>
<td>127</td>
</tr>
</tbody>
</table>

| Upgrade AutoConfigTestConfigurations | 129 |

<table>
<thead>
<tr>
<th>Upgrade file</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update path to 46xxsettings.txt file</td>
<td>70</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Upgrading</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrading test configurations</td>
<td>112</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Upgrading AAWG</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing system layer updates</td>
<td>115</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Upload</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone custom files</td>
<td>63</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Uploading</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Equinox clients</td>
<td>53</td>
</tr>
<tr>
<td>Files on Utility Server</td>
<td>62</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Utility server</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>59</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Utility Server</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activating firmware</td>
<td>69</td>
</tr>
<tr>
<td>Backing up</td>
<td>65</td>
</tr>
<tr>
<td>Backing up phone settings</td>
<td>64</td>
</tr>
<tr>
<td>Capacity</td>
<td>60</td>
</tr>
<tr>
<td>Deactivating firmware</td>
<td>71</td>
</tr>
<tr>
<td>Firmware package</td>
<td>67</td>
</tr>
<tr>
<td>Firmware upgrade is not working</td>
<td>140</td>
</tr>
<tr>
<td>Logging in</td>
<td>61</td>
</tr>
<tr>
<td>Migrating data</td>
<td>128</td>
</tr>
<tr>
<td>Removing firmware</td>
<td>71</td>
</tr>
<tr>
<td>Restoring data</td>
<td>66</td>
</tr>
<tr>
<td>Setting up a DHCP server</td>
<td>60</td>
</tr>
<tr>
<td>Starting</td>
<td>61</td>
</tr>
<tr>
<td>Stopping</td>
<td>61</td>
</tr>
<tr>
<td>Unpacking firmware</td>
<td>68</td>
</tr>
<tr>
<td>Updating path to 46xxsettings.txt file</td>
<td>70</td>
</tr>
<tr>
<td>Uploading files</td>
<td>62</td>
</tr>
<tr>
<td>Uploading phone custom files</td>
<td>63</td>
</tr>
<tr>
<td>Viewing IP phone custom files</td>
<td>63</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>V</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Videos</td>
<td>151</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Viewing</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home location</td>
<td>74</td>
</tr>
<tr>
<td>View published settings</td>
<td>81</td>
</tr>
</tbody>
</table>

| Virtual hardware adjustments | 144 |

<table>
<thead>
<tr>
<th>W</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Watch list</td>
<td>150</td>
</tr>
<tr>
<td>Web administration portal</td>
<td>136</td>
</tr>
<tr>
<td>Not accessible</td>
<td>136</td>
</tr>
<tr>
<td>Web deployment</td>
<td>57</td>
</tr>
<tr>
<td>Client downloading statistics</td>
<td>57</td>
</tr>
<tr>
<td>Web Deployment</td>
<td>53</td>
</tr>
<tr>
<td>Port configuration</td>
<td>53</td>
</tr>
<tr>
<td>Web deployment service</td>
<td>53</td>
</tr>
<tr>
<td>Client downloading statistics</td>
<td>57</td>
</tr>
<tr>
<td>Uploading Avaya Equinox clients</td>
<td>53</td>
</tr>
<tr>
<td>Web Deployment service overview</td>
<td>53</td>
</tr>
</tbody>
</table>