



Administering Avaya Aura[®] Device Services

Release 10.2.x
Issue 14
June 2026

Notices

© 2026 Avaya LLC. All Rights Reserved.

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Hosted Service

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

Licenses

The Global Software License Terms ("Software License Terms") are available on the following website <https://www.avaya.com/en/legal-license-terms/> or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who

installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

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

Virtualization

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

Third Party Components

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](http://www.mpegla.com).

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your

company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction	17
Purpose	17
Changes to platform support	17
Change history	18
Chapter 2: Avaya Aura® Device Services overview	21
New in Avaya Aura® Device Services Release 10.2.1.4	21
New in Avaya Aura® Device Services Release 10.2.1.1	22
New in Avaya Aura® Device Services Release 10.2.1	22
New in Avaya Aura® Device Services Release 10.2.0.1	22
New in Avaya Aura® Device Services Release 10.2	23
Solution topology	23
Automatic configuration flow	24
Components	25
Data retention	27
Data encryption	27
Deployments with Avaya Aura® and without Avaya Aura®	28
Chapter 3: Management of Avaya Aura® Device Services with the web administration portal	30
Logging in to the Avaya Aura® Device Services web administration portal	30
Web administration portal roles	31
Starting or stopping Avaya Aura® Device Services	31
Managing application sessions	32
Application Properties field descriptions	32
Configuring enhanced search options	33
Enabling an external load balancer	34
Certificate management	35
Client certificate policy administration	35
Configuring the client certificate policy using the Avaya Aura® Device Services web administration portal	35
Integration with Avaya Workspaces for Avaya Oceana®	37
Enabling Avaya Breeze® platform authorization	37
Dynamic Configuration service management	38
Messaging server address discovery management	38
LDAP server management	40
Cross-origin resource sharing	41
Enabling Cross-origin resource sharing for the Service Interface	41
Enabling Cross-origin resource sharing for the Administrator Interface	42
Web Deployment service management	43
Scheduling a Cassandra database repair	43

Chapter 4: Avaya Aura® Device Services Single Sign-On management	44
SAML v2.0 and OAuth2 SSO overview	44
Authentication flows	46
Attribute mapping between Keycloak and a third-party identity provider	47
Token authentication realm	48
Access and refresh token expiry times	49
The simultaneous use of multiple identity providers	50
Device Authorization Flow	51
Prerequisites for SSO configuration	52
Prerequisites for SAML v2.0 and OAuth2 SSO configuration	52
Prerequisites for Device Authorization Flow configuration	54
Prerequisites for Workspaces SSO configuration	54
Checklist for SSO authentication configuration	55
Avaya Aura Device Services integration with Microsoft Azure Active Directory	58
Checklist for configuring Microsoft Azure Active Directory integration using SAML v2.0	58
Creating a new application	59
Configuring user and administrator groups	61
Adding users to groups	61
Obtaining the group ID	62
Assigning users and groups to the SSO application on Microsoft Azure	62
Configuring an Azure AD SAML v2.0 identity provider on Keycloak	63
Avaya Aura® Device Services integration with Office 365 using OAuth2	64
Checklist for configuring Office 365 integration using OAuth2	64
Registering an application for SSO purposes	65
Obtaining the application ID	66
Allowing the application to read Microsoft Azure directory data	66
Obtaining the application client secret	67
Adding an Office365 OAuth2 identity provider to Keycloak	67
Disabling the identity provider redirector	68
Adding a hard-coded user role in Keycloak	68
Avaya Aura Device Services integration with Ping Identity	70
Checklist for configuring Ping Identity integration using SAML v2.0	70
Creating a new SAML v2.0 application on Ping Identity	71
Obtaining the XML configuration file	72
Configuring user and administrator Population groups	73
Configuring attribute mapping on Ping Identity	74
Configuring a Ping Identity SAML v2.0 identity provider on Keycloak	75
Creating users on Ping Identity	76
Avaya Aura Device Services integration with OKTA	76
Checklist for configuring OKTA integration using SAML v2.0	76
Creating a new SAML v2.0 application on OKTA	78
Obtaining the XML configuration file	79
Configuring an OKTA SAML v2.0 identity provider on Keycloak	79

Configuring user and administrator groups.....	80
Creating users on OKTA.....	81
Adding users to groups.....	81
Assigning a group to an OKTA SAML application.....	82
Configuring attribute mapping on OKTA.....	82
Avaya Aura Device Services integration with Microsoft AD FS.....	86
Checklist for configuring AD FS integration using SAML v2.0.....	86
Configuring an AD FS SAML v2.0 identity provider on Keycloak.....	88
Configuring Keycloak as a relying party trust.....	88
Configuring the claim issuance policy.....	89
Avaya Aura Device Services integration with One Login.....	90
Checklist for configuring OneLogin integration using SAML v2.0.....	90
Creating a new SAML v2.0 application on OneLogin.....	92
Configuring a OneLogin SAML v2.0 identity provider on Keycloak.....	93
Configuring attribute mapping on OneLogin.....	93
Creating users on OneLogin.....	94
Avaya Aura Device Services integration with IBM SVA.....	95
Checklist for configuring IBM SVA integration using SAML v2.0.....	95
Creating a new SAML v2.0 application on IBM SVA.....	96
Configuring an IBM SVA SAML v2.0 identity provider on Keycloak.....	98
Configuring user and administrator groups.....	98
Assigning groups to your IBM SVA SAML application.....	99
Configuring attribute mapping on IBM SVA.....	100
Creating users on IBM SVA.....	101
Adding users to groups.....	101
Avaya Aura Device Services integration with Duo.....	102
Checklist for configuring Duo integration using SAML v2.0.....	102
Creating a new SAML v2.0 application on Duo.....	103
Adding your SAML application to the Duo Access Gateway.....	104
Configuring a Duo SAML v2.0 identity provider on Keycloak.....	105
Avaya Aura Device Services integration with Imprivata.....	106
Checklist for configuring Imprivata integration using SAML v2.0.....	106
Configuring LDAP settings.....	107
Enabling role fetching from LDAP.....	107
Configuring an Imprivata SAML v2.0 identity provider on Keycloak.....	108
Downloading the SPSSODescriptor file from Keycloak.....	108
Avaya Aura Device Services integration with Auth0.....	109
Checklist for configuring Auth0 integration using SAML v2.0.....	109
Creating a new application.....	110
Configuring an Auth0 SAML v2.0 identity provider on Keycloak.....	112
Creating users on Auth0.....	113
Setting up last name and first name attributes in the user's profile.....	114
Device Authorization flow configuration.....	115

Checklist for device flow configuration.....	115
Creating client mapping for the device flow.....	116
Publishing COMM_ADDR_HANDLE parameters for J1XX phones.....	118
Workspaces SSO Flow configuration.....	118
Checklist for Workspaces SSO Flow configuration.....	119
Creating client mapping for the Workspaces SSO Flow.....	119
Switching to another identity provider.....	120
Checklist for switching to another identity provider.....	121
Deleting users from Keycloak.....	121
Disabling an identity provider.....	121
Changing the identity provider redirector.....	122
Logging in to the Keycloak web administration portal.....	122
Changing your Keycloak password.....	123
Authorization realm configuration on UC servers and Avaya Workplace Client.....	123
Configuring Keycloak settings.....	124
Starting and stopping the Keycloak service.....	126
Obtaining the client secret.....	126
Creating client mapping.....	126
Managing an existing client mapping.....	128
Configuring a time interval for updating public keys in client mappings.....	129
Regenerating the Keycloak client secret.....	129
Updating the identity provider mapping.....	130
Importing third-party identity provider private CA certificates.....	130
Importing a third-party identity provider.....	131
Selecting the default identity provider	132
Disabling the default identity provider.....	133
Modifying the attribute mapping between the third-party identity provider and Keycloak.....	133
Attribute mapping parameters for Office 365 OAuth2 identity provider.....	136
Attribute mapping parameters for Microsoft Azure SAML v2.0 identity provider.....	136
Attribute mapping parameters for Ping Identity SAML v2.0 identity provider.....	137
Attribute mapping parameters for OKTA SAML v2.0 identity provider.....	138
Attribute mapping parameters for ADFS SAML v2.0 identity provider.....	138
Attribute mapping parameters for OneLogin SAML v2.0 identity provider.....	139
Attribute mapping parameters for the IBM SVA SAML v2.0 identity provider.....	139
Attribute mapping parameters for the Duo SAML v2.0 identity provider.....	140
Attribute mapping parameters for Imprivata SAML v2.0 identity provider.....	141
Attribute mapping parameters for Auth0 SAML v2.0 identity provider.....	141
Checklist to Configure Keycloak using a secure LDAP	142
Obtaining LDAP Server Certificate.....	142
Importing the Certificate into the Keycloak Truststore.....	143
Configuring LDAPS in Keycloak.....	144
Configuring the LDAP UID mapping.....	144
Synchronizing data between Avaya Aura [®] Device Services and an identity provider.....	145

Testing the integration with an identity provider from the Google Chrome web browser.....	146
Testing the integration with the identity provider from the web administration portal.....	147
OAuth2 testing status.....	148
Configuring access and refresh token expiry times.....	149
Blocking access to the Avaya Authorization service.....	151
Enabling OAuth database replication in a cluster environment.....	151
Keycloak log management.....	152
Chapter 5: Avaya Spaces integration.....	153
Checklist for configuring Avaya Spaces integration.....	153
Avaya Spaces account configuration.....	154
Setting up a company and domain in Avaya Spaces.....	154
Creating an API key.....	155
The use of Enterprise SSO for Avaya Spaces integration.....	155
Obtaining an API key and API key secret.....	156
Setting up Avaya Spaces integration.....	156
Configuring data synchronization between Avaya Aura® Device Services and Avaya Spaces....	158
Stopping synchronization with Avaya Spaces.....	159
Phone number synchronization.....	160
Configuring phone number synchronization.....	160
Uploading Avaya Spaces language and time zone settings to Avaya Aura® Device Services....	161
Language file format.....	162
Time zone file format.....	163
User and license management overview.....	163
Avaya Spaces user licenses.....	164
Adding enterprise users for registration on Avaya Spaces.....	165
Registering enterprise users on Avaya Spaces.....	166
Removing an unregistered user.....	167
Automatic registration of LDAP group members on Avaya Spaces.....	168
Avaya Spaces user management.....	172
Cancelling user registration and license upgrade operations	178
Updating Avaya Spaces integration parameters.....	179
Avaya Spaces integration settings.....	179
Disabling Avaya Spaces integration.....	180
Deleting the Avaya Spaces configuration.....	181
Viewing the Avaya Spaces connection status.....	181
Configuring Avaya Spaces SSO for Avaya Spaces clients.....	182
Chapter 6: LDAP server management.....	183
Configuring the UID mapping attributes when using multiple authentication domains.....	184
Adding a new enterprise LDAP server.....	184
Enterprise LDAP Server Configuration field descriptions.....	186
Configuring additional base context DN.....	193
LDAP server discovery using DNS SRV records.....	194
Checklist for configuring LDAP discovery using DNS SRV records.....	195

Configuring LDAP server discovery using DNS SRV records.....	196
Testing connection to an LDAP server.....	197
Modifying the provenance priority.....	198
Administering the LDAP server configuration.....	198
Enabling LDAP authentication for OAuth.....	199
Modifying enterprise directory attribute mappings.....	199
Configuring Windows Authentication for Active Directory.....	200
Selecting an authentication domain.....	202
Setting up user synchronization with the LDAP server.....	202
Stopping synchronization with the LDAP server.....	203
LDAP user deletion confirmation.....	204
Enabling the LDAP user deletion policy.....	205
Managing LDAP users pending deletion.....	205
Disabling the LDAP user deletion policy.....	206
Configuring the internationalization parameters.....	206
Adding a trusted host.....	207
Supported characters for LDAP attributes.....	208
Updating user attributes in LDAP.....	208
Open LDAP user data imports.....	209
Structure of a CSV file for the bulk upload procedure.....	209
Uploading users in bulk.....	211
Changing the PictureURL attribute.....	211
Configuration of LDAP contact search.....	212
Selecting LDAP servers for the contact search.....	213
Setting up contact search for additional base context DNSs.....	213
Limiting the contact search scope to user's own group or department.....	214
Limiting the System Manager contact search	215
Disabling contact search for a LDAP server.....	215
Chapter 7: Avaya Aura[®] Device Services network settings configuration	217
Avaya Aura [®] Device Services network configuration checklist.....	218
Prerequisites for configuring Avaya Aura [®] Device Services network settings.....	219
Configuring network settings using the cliChangeNet.sh script.....	220
Configuring network settings using the Avaya Aura [®] Device Services configuration utility.....	221
Chapter 8: Certificate management	225
Managing certificates in the Avaya Aura [®] Device Services web administration portal.....	225
Generating System Manager identity certificates.....	225
Managing identity certificates.....	226
Managing CSRs.....	227
Managing keystore data.....	230
Configuring expiration notifications for identity certificates.....	231
Managing server interface certificates.....	232
Managing truststore certificates.....	233
Certificate revocation management.....	233

Configuring the revocation check policy.....	235
Importing the secure LDAP certificate using the web administration portal.....	235
Importing third-party CA-signed certificates.....	236
Chapter 9: Web Deployment service management.....	239
Web Deployment port configuration.....	239
Uploading the client installer.....	240
Appcast items field descriptions.....	242
Editing an appcast item.....	243
Selecting interactive or non-interactive upgrade mode for Avaya Workplace Client for Windows	243
Deleting an appcast item.....	244
Reviewing download statistics.....	245
Download statistics field descriptions.....	245
Chapter 10: Utility Server administration.....	246
Utility Server capacity limits.....	247
Supported and unsupported phone models.....	247
Setting up a DHCP server.....	249
Starting and stopping the Utility Server.....	249
Enabling access to the Utility Server using an HTTP connection.....	250
Logging in to the Utility Server.....	250
Reviewing the disk space occupied by firmware package files.....	251
Increasing the file size limit for phone firmware packages to 1.5 GB.....	252
Uploading files on the Utility Server.....	252
Uploading settings file to the Utility Server.....	253
Uploading an IP phone custom file.....	254
Viewing custom files uploaded on the Utility Server.....	255
Accessing IP phone custom files.....	255
Backing up H.323 phone settings on the Utility Server.....	256
PhoneBackup Feature Configuration.....	257
Utility Server backup and restore.....	258
Backing up data stored on the Utility Server.....	258
Restoring the Utility Server data.....	259
Backup and restore of “phone model to group ID” mapping	259
Firmware management.....	259
Viewing firmware packages available on the Utility Server.....	260
Unpacking a firmware package.....	261
Activating a firmware package.....	262
Deactivating a firmware package.....	263
Removing a firmware package.....	264
Chapter 11: Administration of the Dynamic Configuration service.....	265
Considerations for administering SIP parameters in an environment without Avaya Aura®	267
Viewing the Home location in System Manager.....	268
Dynamic configuration setting priorities.....	268
Assigning a group identifier to a phone model.....	269

Adding a new platform.....	270
Deleting a platform.....	270
Creating a new configuration.....	271
Configuration field descriptions.....	271
Configuration settings.....	273
Password masking.....	273
Avaya Aura® Device Services specific parameters.....	274
Overwriting an existing configuration.....	275
Testing configuration settings.....	276
Publishing the configuration settings.....	276
Viewing published settings.....	278
Retrieving configuration settings for a user.....	279
Import of dynamic configuration settings.....	279
Importing dynamic configuration settings using a file in the JSON format.....	279
Importing parameter values from a 46xxsettings.txt file.....	282
Bulk imports.....	282
Managing automatic logging in to Avaya clients.....	285
Administering the default configuration.....	286
Defaults field descriptions.....	287
Split Horizon DNS mapping.....	288
Mapping the IP address to the FQDN.....	288
Enabling Split Horizon DNS mapping.....	289
Split Horizon DNS Mapping field descriptions.....	289
Chapter 12: Integrated Windows Authentication administration and management.....	290
Authentication prerequisites.....	290
Setting up the Windows Domain Controller.....	291
Windows Domain Controller command descriptions.....	293
Enabling encryption for the domain user.....	293
Setting up IWA on the Avaya Aura® Device Services administration portal.....	294
Chapter 13: AWS-specific management options.....	297
Updating an existing stack with a new CloudFormation template.....	297
Chapter 14: Cassandra clustering configuration on Avaya Aura® Device Services.....	298
Scheduling a Cassandra database repair.....	299
Assigning a node to a different Cassandra datacenter.....	300
Reviewing the Cassandra database status.....	301
Configuring an additional seed node.....	302
Chapter 15: Security options.....	303
Configuring the data retention period.....	303
Antivirus support.....	303
Prerequisites for installing antivirus software.....	304
Changing the SELinux mode to “permissive”.....	304
File access privileges.....	305
Data encryption management.....	306

Enabling or disabling disk encryption on Avaya Aura® Device Services.....	306
Remote key server management.....	307
Passphrase management.....	308
Viewing data encryption status.....	310
Local key store management.....	311
Advanced Intrusion Detection Environment tool management.....	311
Creating a baseline database.....	312
AIDE scanning.....	313
Reviewing the AIDE scanning report.....	316
Enabling additional STIG hardening.....	317
Disabling additional STIG hardening.....	317
Transport Layer Security overview.....	318
Selecting a minimum TLS version.....	319
Configuring UEFI Secure Boot for OVA-based virtual machines.....	320
Checking the UEFI Secure Boot status.....	320
Configuring the SameSite cookie attribute.....	321
Configuring the SameSite attribute for web-based clients.....	322
Characters supported for Avaya Aura® Device Services passwords.....	323
Password policy for human-user accounts.....	323
Configuring password rules.....	324
Avaya Aura® Device Services entry points.....	324
HTTP Proxy.....	325
Chapter 16: Monitoring options.....	326
Monitoring cluster nodes.....	326
Cluster Nodes field descriptions.....	326
Checking the Avaya Aura® Device Services status from the CLI.....	327
Checking the status of a remote Avaya Aura® Device Services node from the CLI.....	328
Enabling or disabling HTTPS for health checks.....	329
Viewing performance statistics.....	329
Performance charts.....	330
Logs.....	332
Log management.....	332
Configuring remote logging.....	332
Monitoring Avaya Aura® Device Services logs.....	333
Changing a logging level.....	334
Scheduling log collection	335
Downloading logs.....	336
Alarms.....	337
Alarms configuration for System Manager.....	338
Alarms configuration for a third-party SNMP server.....	340
Avaya Aura® Device Services alarms list.....	342
Enhanced Access Security Gateway for real time support.....	349
Enabling the Enhanced Access Security Gateway from the CLI.....	349

Removing EASG.....	350
Chapter 17: Backup and restore.....	351
Backing up Avaya Aura® Device Services.....	351
Automatic backups.....	352
Configuring automatic backups.....	353
Changing the location of automatic backups.....	354
Retrieving Cassandra database username and password.....	355
Locating keystore password.....	355
Avaya Aura® Device Services configuration portability.....	356
Exporting the configuration file using the web administration portal.....	356
Exporting the configuration file using the CLI.....	357
Preparing the exported configuration file for silent installation.....	358
Restoring options for standalone and cluster environments.....	358
Restoring Avaya Aura® Device Services in a standalone environment.....	358
Restoring an Avaya Aura® Device Services cluster.....	360
Synchronizing client ID.....	364
Chapter 18: Avaya Aura® Device Services upgrade and migration operations.....	365
Avaya Aura® Device Services upgrade checklist.....	366
Avaya Solutions Platform migration considerations.....	367
Upgrading Avaya Solutions Platform from Release 4.0 to 5.0.....	367
System layer (operating system) updates for virtual machines deployed using Avaya-provided OVA.....	368
Checklist for updating the system layer.....	368
Determining if a system update is applicable.....	368
Downloading, extracting, and staging a system layer update.....	369
Installing a staged system layer update.....	370
Updating the system layer for software-only deployments.....	371
Upgrading Avaya Aura® Device Services.....	372
Creating a full system backup.....	373
Upgrading the Avaya Aura® Device Services application.....	373
Rolling back the upgrade.....	376
Upgrading Avaya Aura® Device Services on AVP.....	377
Preparing for an AVP upgrade.....	379
Upgrading the Avaya Aura® Device Services application on AVP virtual machines.....	381
Deploying new AVP virtual machines.....	383
Completing the upgrade.....	384
Rolling back the AVP upgrade.....	385
Configuring RSA public and private keys for SSH connections in a cluster.....	387
Migrating Utility Server data.....	388
Upgrading existing test configurations.....	389
Running a patch to allow Avaya Workplace Client for Windows to connect to the Web Deployment service.....	389

Running a patch to allow the Avaya Aura® Web Gateway to connect to the Avaya Aura® Device Services automatic configuration service.....	391
Enabling Open LDAP replication.....	391
Re-enabling Open LDAP replication after removing a node from a cluster.....	392
Checking for DRS synchronization.....	393
Setting up user synchronization with LDAP after deployment.....	394
Chapter 19: Upgrading RHEL 8.4 to RHEL 8.10 on OVA- based virtual machines.....	395
Chapter 20: Troubleshooting.....	397
Avaya Workspaces Client cannot connect to Avaya Aura® Device Services.....	397
Troubleshooting for the DRS service.....	398
DRS remains in Ready to Repair state.....	398
DRS remains in repairing state for a long time.....	398
DRS remains in not polling state.....	398
DRS fails with constraint error.....	399
Avaya Aura® Device Services installation or upgrade fails due to invalid System Manager certificates.....	399
Services are not working properly after an installation or upgrade.....	400
EASG login using craft username results in an Access Denied error.....	400
Admin user is not prompted for password in sudo su.....	401
ESG cannot connect to Avaya Aura® Device Services.....	401
A new private key failed to generate.....	401
DNS entries disappear from the /etc/resolv.conf file after restarting Avaya Aura® Device Services.....	402
Check for Updates feature is not working.....	403
Slow Avaya Aura® Device Services performance.....	403
Primary System Manager fails.....	403
Cannot connect to System Manager after replacing a revoked System Manager certificate with a valid certificate.....	404
Unable to access the web administration portal when the primary node Session Manager is non-operational.....	405
PPM certificate error	405
Repairing faulty users.....	406
Exception in the AADS.log file.....	407
The AADS.log file contains contact integrity data.....	407
System Manager does not show Avaya Aura® Device Services alarms.....	407
Firmware upgrade fails for certain endpoints.....	409
Cannot upload phone firmware packages larger than 800 MB to the Utility Server after the upgrade.....	409
Synchronization with the LDAP server fails.....	409
Open LDAP replication fails.....	410
Open LDAP replication fails if Avaya Aura® Device Services uses a custom identity certificate for server interfaces.....	410
Allocating unused disk space to logical volumes.....	411
ESXi virtual hardware adjustments.....	413

Increasing the virtual disk size of AWS virtual machines.....	415
Cannot reinstall a non-seed node due to Cassandra startup error.....	417
Troubleshooting for OAuth2 authorization.....	417
OAuth2 authentication does not work as expected.....	417
Login page for the third-party identity provider is not displayed.....	417
An error page is displayed instead of the Login page.....	418
Login credentials do not work.....	418
Avaya Workplace Client displays an authentication error.....	419
Users cannot log in to their clients or phones using SSO.....	420
A test user cannot log in to the identity provider.....	420
Interoperability issues between Avaya Aura® Device Services and the third-party identity provider.....	421
Avaya Spaces integration.....	422
Avaya Spaces connectivity errors.....	422
Avaya Aura® Device Services does not contain the latest Avaya Spaces CA certificate.....	423
Cannot register an enterprise user on Avaya Spaces.....	424
Avaya Spaces user management operation fails.....	425
Avaya Spaces pages blocked.....	425
Logs collected using the collectlogs command are encrypted.....	426
Avaya Workplace Client cannot connect to Avaya Aura® Device Services.....	426
Avaya Workplace Client cannot connect to Avaya Aura® Device Services when the secure connection is enabled.....	427
Cannot access Avaya Aura® Device Services resources over port 443.....	427
The location of automatic backups has changed after the upgrade.....	428
Disk space full on one node disables the service on all nodes.....	428
Running the Cassandra repair manually.....	429
Auto Configuration Failure: 500 Internal Server Error.....	429
RHEL single-user mode.....	430
Booting the RHEL into single-user mode.....	430
Changing the password for single-user mode.....	431
Exiting the single-user mode.....	432
Client login failure when Identity provider link already exists in Keycloak.....	432
Secured LDAP user federation with keycloak error occurs during configuration settings.....	433
Users cannot log in to the client due to expiry of third-party Identity provider certificate.....	434
Chapter 21: Migrating Avaya Aura® Device Services from VMware to ASP R6.0.x (KVM on RHEL 8.10).....	435
Migrating Avaya Aura® Device Services from VMware to ASP R6.0.x (KVM on RHEL 8.10).....	435
Obtaining existing VMware details.....	436
Checklist of prerequisite tasks to migrate Avaya Aura® Device Services from VMware to ASP R6.0.x (KVM on RHEL 8.10).....	436
Obtaining Avaya Aura® Device Services network configuration details.....	437
Chapter 22: Resources.....	439
Documentation.....	439

Finding documents on the Avaya Support website.....	440
Avaya Documentation Center navigation.....	440
Viewing Avaya Mentor videos.....	442
Support.....	442
Using the Avaya InSite Knowledge Base.....	443
Appendix A: Additional administration tools.....	444
collectlogs.....	445
clitool-acs.....	446
statusAADS utility.....	446
Checking the Avaya Aura® Device Services status from the CLI.....	447
Shutting down Avaya Aura® Device Services gracefully.....	447
System layer commands.....	448
sys secconfig command.....	449
sys versions command.....	450
sys volmgt command.....	450
sys smcvemgt command.....	454
sys ipv6config command.....	457
passwdrules command.....	458
Data encryption commands.....	460
runUserDiagnostics tool.....	462
enableVantageFWSupport.sh command.....	463
https_healthCheck.sh command.....	463
Aliases.....	464
app commands.....	464
cdto commands.....	465
Using the Tmux utility.....	466
Glossary.....	467

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*.

Changes to platform support

As of January 1, 2026, Avaya has refined its infrastructure support strategy for Avaya Aura® and Surround Applications. This update specifically impacts Software-Only and Infrastructure as a Service (IaaS) deployment models. To ensure your environment remains compliant and supported, review the following changes to supported platforms:

Discontinued Platforms:

- Hypervisor: Microsoft Hyper-V
- Cloud Platforms: Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud

Supported platforms for Software Only and Infrastructure as a Service (IaaS) deployment models:

- Cloud Platform: AWS
- On-premises platforms: KVM, Nutanix, VMware

Change history

Issue	Date	Summary of changes
14	June 2026	Added the following sections for R10.2.1.4: • New in Avaya Aura Device Services Release 10.2.1.4 on page 21 • Retrieving Cassandra database username and password on page 355 • Locating keystore password on page 355 • Synchronizing client ID on page 364 • Client login failure when Identity provider link already exists in Keycloak on page 432 • Secured LDAP user federation with keycloak error occurs during configuration settings on page 433 • Users cannot log in to the client due to expiry of third-party Identity provider certificate on page 434 Updated the following sections for R10.2.1.4: • Backing up Avaya Aura Device Services on page 351 • LDAP server management on page 183 • Enterprise LDAP Server Configuration field descriptions on page 186
13	March 2026	Added the section: • Changes to platform support on page 17
12	January 2026	Updated the following section: • Avaya Spaces integration on page 153
11	October 2025	Added the following sections: • PhoneBackup Feature Configuration on page 257 • Disabling PhoneBackup Feature or Whitelist Custom IP Range on page 257 • Verifying the Configuration Status of PhoneBackup on page 258 • Rolling Back Changes in PhoneBackup Feature on page 258
10	August 2025	Updated the following section: • Avaya Aura Device Services alarms list on page 342

Issue	Date	Summary of changes
9	April 2025	Added the following sections: • New in Avaya Aura Device Services Release 10.2.1.1 on page 22 • Limiting the System Manager contact search on page 215 • HTTP Proxy on page 325 Updated the following sections: • Uploading the client installer on page 240 • Setting up the Windows Domain Controller on page 291
8	March 2025	Added the following sections: • Checklist to Configure Keycloak using a secure LDAP on page 142 • Obtaining LDAP Server Certificate on page 142 • Importing the Certificate into the Keycloak Truststore on page 143 • Configuring LDAPS in Keycloak on page 144
7	January 2025	Removed the following topic: • Registering an Avaya Spaces Avaya Cloud account
6	December 2024	Added the following sections for Release 10.2.1: • New in Avaya Aura® Device Services Release 10.2.1 • Upgrading RHEL 8.4 to RHEL 8.10 on OVA- based virtual machines • Checklist to migrate Avaya Aura® Device Services from VMware to KVM • Migrating AADS from VMware to ASP R6.0.x (KVM on RHEL 8.10) • Prerequisites for Device Authorization Flow configuration
5	August 2024	Updated the following section: Disk space full on one node disables the service on all nodes on page 428
4	July 2024	Updated the following section: Supported and unsupported phone models on page 247
3	May 2024	Updated the following section: Enterprise LDAP Server Configuration field descriptions on page 186

Issue	Date	Summary of changes
2	May 2024	Added the following section: Auto Configuration Failure: 500 Internal Server Error on page 429 Updated the following sections: New in Avaya Aura Device Services Release 10.2 on page 23 Keycloak log management on page 152 Changing a logging level on page 334
1	December 2023	Release 10.2.

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. It can also provide file server capabilities, such as 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 Workplace Client. This document also uses the term “client” when referring to Avaya Workplace Client.

SIP endpoints, such as Avaya Workplace Client, 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 Workplace Client 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 Workplace Client, you cannot manually force the software to update unless it is configured through Avaya Aura® Device Services.

New in Avaya Aura® Device Services Release 10.2.1.4

The following is the change introduced in Release 10.2.1.4 of Avaya Aura® Device Services:

- Added support to the new Enterprise-Directory Type, ActiveDirectory_2025.

New in Avaya Aura® Device Services Release 10.2.1.1

Avaya Aura® Device Services Release 10.2.1.1 supports the following new features and enhancements:

System Manager contacts filtration

With Release 10.2.1.1, Avaya Aura® Device Services restrict the display of contacts specific to System Manager upon searching the contacts.

HTTP Proxy support for client ID mapping

With Release 10.2.1.1, Avaya Aura® Device Services support HTTP Proxy configuration for client ID mapping.

Addition of a new ED signature for macOS

With Release 10.2.1.1, the Avaya Aura® Device Services support adding ED signature for macOS binary upload.

New in Avaya Aura® Device Services Release 10.2.1

Avaya Aura® Device Services Release 10.2.1 supports the following new features and enhancements:

Support for Software-Only Deployment on Nutanix Environment

With Release 10.2, Avaya Aura® Device Services Software-Only application can be deployed on Nutanix 6.5 and later.

Red Hat Enterprise Linux 8.10 support for Avaya Aura® Device Services

With Release 10.2.1, Avaya Aura® Device Services supports Red Hat Enterprise Linux Release 8.10.

Kernel-based Virtual Machine (KVM) on RHEL 8.10 hypervisor support

With Release 10.2, Avaya Aura® Device Services can be deployed on Avaya-supplied KVM on RHEL Release 8.10 hypervisor (Avaya Solutions Platform 130 R6.0).

Keycloak with FIPS support

With Release 10.2.1 Avaya Aura® Device Services provide Keycloak with FIPS support.

New in Avaya Aura® Device Services Release 10.2.0.1

The following is a summary of changes in Release 10.2.0.1 of Avaya Aura® Device Services:

- Added support to a new Enterprise-Directory Type, ActiveDirectory_2022.
- Rollback to previous AADS version below 10.2.0.1 is not supported.

New in Avaya Aura® Device Services Release 10.2

The following is a summary of new functionalities added to Avaya Aura® Device Services in Release 10.2:

Enable/Disable logging

- Before Release 10.2, AADS supported extended logging at the system level only. With AADS Release 10.2, you can enable or disable logging at an individual user level.
- LOG_VERBOSITY property is added in the AADS dynamic configuration at a user level.

Support for VMware 8.0

With Release 10.2, Avaya Aura® applications support the VMware® vSphere ESXi 8.0 and VMware® vCenter Server 8.0 in a VMware virtualized environment.

Client ID configuration

Before Release 10.2, client ID used by J100 phones was hard-coded in AADS and couldn't be configurable. With Release 10.2, you can configure the client-id in AADS, which enables IAM to apply customer-specific requirements in the access token when the client authenticates.

Dynamic configuration for telecommuter number

Using AADS auto-config service API, the administrator can configure the telecommuter number and associate it with agents using Workplace. With this release, only one telecommuter number is supported.

Upgraded Keycloak version

Upgraded Keycloak version from Release 6.0.1 to Release 22.0.4.

Added MS Graph API support

AADS now supports MS Graph API as a replacement for MS Azure API, which Microsoft retired this year.

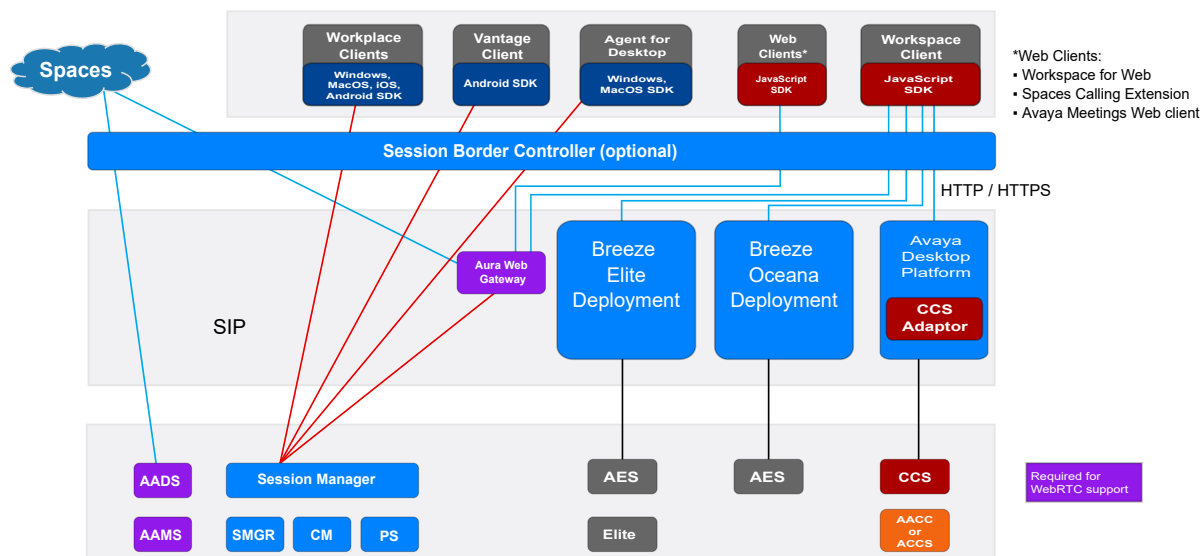
For more information on MS Graph API replacing MS Azure API, see PSN at <https://download.avaya.com/css/public/documents/101086282> for details.

Note:

Microsoft announced EoS for Azure AD Graph API. MS Graph API will replace Azure AD Graph API.

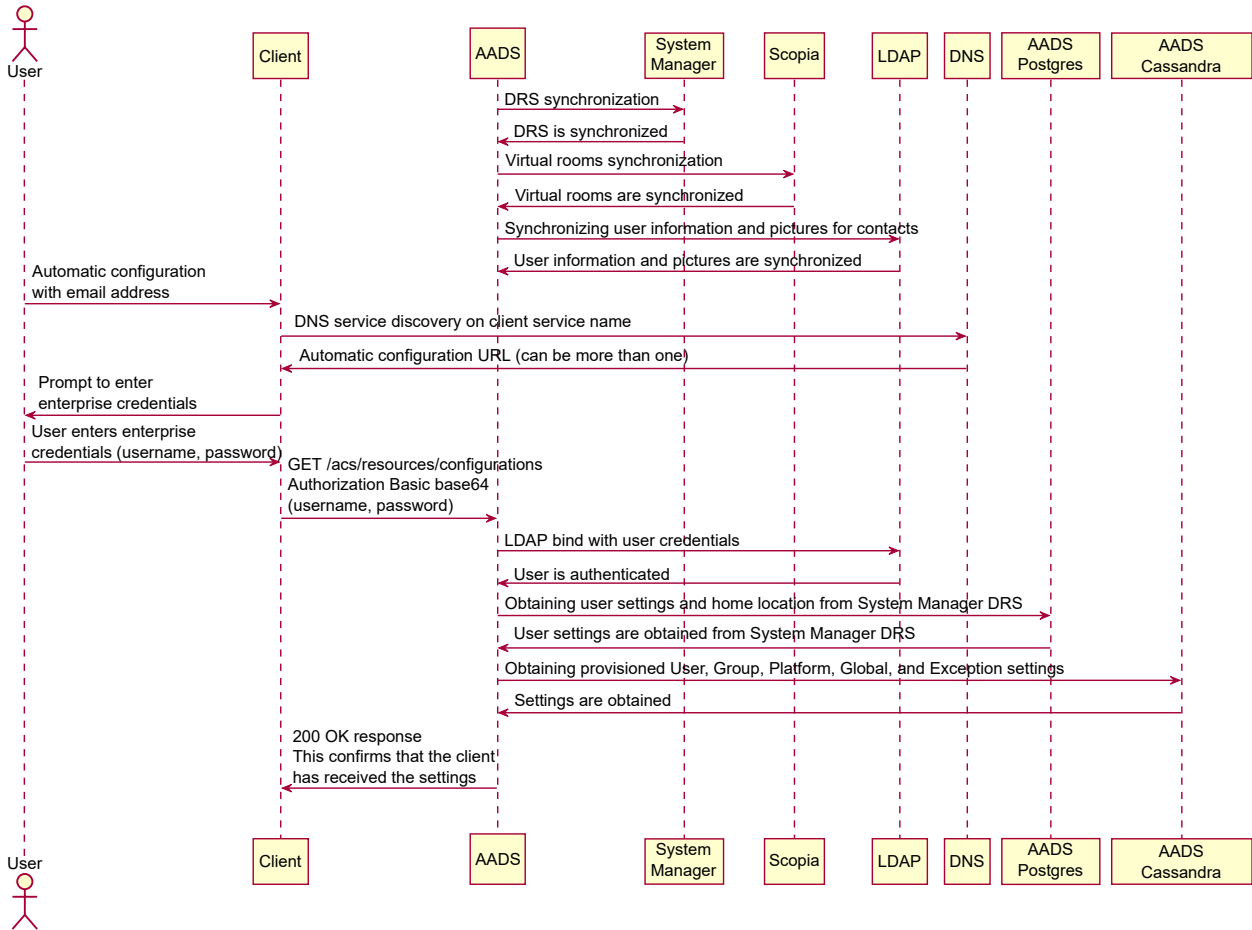
Solution topology

The following diagram shows a solution with Avaya Aura® Device Services.



Automatic configuration flow

The following diagram shows the automatic client configuration flow.



Components

The following table lists key components that Avaya Aura® Device Services requires. Avaya Aura® Device Services can also integrate with other products and solutions, such as Avaya Workplace Client, Avaya Spaces, and Avaya Workspaces for Avaya Oceana®. 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	Description
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.  Note: Avaya Aura® Device Services does not support the System Manager Geographic Redundancy mode. • 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.  Note: Starting from Release 10.1.1, you can deploy Avaya Aura® Device Services in an environment without Avaya Aura®. When deployed in an environment without Avaya Aura®, Avaya Aura® Device Services does not require Avaya Aura® solution components.
Avaya Session Border Controller (Avaya SBC)	Avaya SBC 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	Description
ESXi Host	A virtual machine running the ESXi Hypervisor software.
ESXi Hypervisor	A platform that runs multiple operating systems on a host computer simultaneously.
vSphere Client	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.
vCenter Server	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.
Avaya Solutions Platform	A platform that is a customized OEM version of VMware ESXi. With Avaya Solutions Platform, customers can run any combination of supported applications on Avaya-supplied servers. Avaya Solutions Platform provides greater flexibility in scaling customer solutions to individual requirements.

Virtualized components	Description
Solution Deployment Manager	The centralized software management solution of Avaya that provides deployment, upgrade, migration, and update capabilities for the Avaya Aura® virtual applications.
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
- Avaya Solutions Platform

Data retention

The following Avaya Aura® Device Services locations can contain private or sensitive user data:

- Log files.
- Avaya Aura® Device Services Cassandra database.

To maximize data privacy and security, you can specify how long you want to keep log files and user data on Avaya Aura® Device Services from the Data Retention page.

Data retention — log files

Avaya Aura® Device Services encrypts all log files that can contain personal information if they are older than the configured retention period.

Data retention — Cassandra database

When a user is deleted from data sources, such as the enterprise LDAP directory, iView, or System Manager, Avaya Aura® Device Services deletes the corresponding records for that user from the Cassandra database after the retention period elapses. The process of deleting data can take up to one hour. For example, if the retention period is one day and the user is deleted from the LDAP directory today, then the user information is removed from the Cassandra database within 24 hours.

Related links

[Configuring the data retention period](#) on page 303

Data encryption

You can enable or disable data encryption when deploying the Avaya Aura® Device Services OVA. When data encryption is enabled, all operational data and log files are encrypted.

You can only enable data encryption on Avaya Aura® Device Services if you use Avaya Solutions Platform or a VMware Virtualized Environment. For software-only deployments, you must enable data encryption on the virtualization platform itself. For more information about enabling data encryption on Amazon Web Services, see [How to Protect Data at Rest with Amazon EC2 Instance Store Encryption](#).

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

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

Encryption of Avaya Aura® Device Services partitions

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

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

The sda boot disk is always unencrypted.

Related links

[Data encryption management](#) on page 306

Deployments with Avaya Aura® and without Avaya Aura®

Starting from Release 10.1.1, you can choose whether Avaya Aura® Device Services requires Avaya Aura® components, such as System Manager or Session Manager, to operate. Avaya Aura® Device Services supports the following deployment options:

- Avaya Aura® deployments, where Avaya Aura® Device Services requires the functionality that Avaya Aura® components provide, such as System Manager or Session Manager. Avaya Aura® Device Services cannot operate if your environment does not include these components.
- Deployments without Avaya Aura®, where Avaya Aura® Device Services does not require any Avaya Aura® components and operates as an independent server. Your environment can include other Avaya Aura® components, but Avaya Aura® Device Services do not use them by default.

You can choose the deployment type when installing the Avaya Aura® Device Services application on a virtual machine. The initial virtual machine deployment process remains the same for both deployment options.

! Important:

You cannot switch the deployment type after installing Avaya Aura® Device Services or when you upgrade Avaya Aura® Device Services to the latest release. To switch to another deployment type, uninstall the Avaya Aura® Device Services application and select the required deployment type when reinstalling Avaya Aura® Device Services.

Considerations and limitations

Avaya Aura® Device Services deployed in an environment without Avaya Aura® cannot use features that System Manager or Session Manager provide. Therefore, certain features work differently in deployments with Avaya Aura® and deployments without Avaya Aura®. For example:

- Identity certificates for Avaya Aura® Device Services interfaces and internode communication. In Avaya Aura® deployments, Avaya Aura® Device Services by default uses identity certificates signed by the System Manager. In deployments without Avaya Aura®, System Manager is unavailable, so you must obtain and use identity certificates provided by a third-party CA.
- Dynamic configuration service. In Avaya Aura® deployments, Avaya Aura® Device Services automatically retrieves certain endpoint configuration settings from System Manager. In deployments without Avaya Aura®, you must manually configure and publish these settings on Avaya Aura® Device Services.
- Alarms. When operating, Avaya Aura® Device Services can trigger various alarms. In Avaya Aura® deployments, you can view these alarms on System Manager. In deployments without Avaya Aura®, you must configure a separate SNMP server to view Avaya Aura® Device Services alarms.
- LDAP and contact search. In deployments without Avaya Aura®, Avaya Aura® Device Services does not perform contact search on System Manager and does not synchronize LDAP data with System Manager.

Deployments without Avaya Aura® do not support the following Avaya Aura® components and their features:

- System Manager and all its features, such as data center topology configuration or DRS synchronization.
- Session Manager and all its features, such as Session Manager Cassandra clustering.

If deployments without Avaya Aura® do not support a particular feature or require a specific setup for a feature, this document mentions it explicitly.

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.

Note:

The System Manager login option is not available if Avaya Aura[®] Device Services is deployed in an environment without Avaya Aura[®].

Before you begin

- In the DNS, add an entry to map the 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`.

Procedure

1. Open your web browser.
2. Type the URL in one of the following formats:

- `https://<FQDN>:8445/admin/`
- `https://<IP_Address>:8445/admin/`

If IPv6 support is enabled you can use either IPv4 or IPv6 addresses.

The following are URL examples:

- IPv4 address example: `https://192.0.2.44:8445/admin`
- IPv6 address example: `https://[2001:db8::7334]:8445/admin`

3. Press **Enter**.

If your browser does not have a valid security certificate, the browser 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.

 Note:

If OAuth is enabled on Avaya Aura® Device Services and LDAP authentication for OAuth is disabled, then you must use the credentials of the administrative user created during OVA deployment. For more information about enabling LDAP authentication, see [Enabling LDAP authentication for OAuth](#) on page 199.

6. Click **Log on**.

Related links

[Web administration portal roles](#) on page 31

Web administration portal roles

Role	Description
Administrator	Enables full access to most web administration portal pages except for the Security Settings page. You can perform any administration operation on the pages you can access.
Services Administrator	
Security Administrator	Enables full access to all web administration portal pages, including the Security Settings page. You can perform any administration operation with this role.
Auditor	Provides read-only access to web administration portal pages. You cannot modify any settings.
Services Maintenance and Support	

Related links

[Logging in to the Avaya Aura Device Services web administration portal](#) on page 30

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 32.
3. Click **Save**.

Application Properties field descriptions

Name	Description
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 10 minutes.
Application HTTPSession Timeout (minutes)	The timeout period for application components. You can enter a value between 1 and 60 minutes. The default value is 15 minutes.
Maximum Concurrent HTTP Sessions	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.

Name	Description
Concurrent HTTP Sessions per User	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.

Configuring enhanced search options

About this task

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

Before you begin

- If you use Avaya Aura® Device Services in an Avaya Aura® environment, on System Manager, configure the mapping from the LDAP directory server to System Manager for the department and city attributes. For example:

Attribute Parameters

Add Mapping

objectGUID	->	sourceUserKey	
userPrincipalName	->	loginName	
sn	->	surname	
mail	->	Microsoft Exchange Handle	Remove
description	+	User Provisioning Rule	Remove
telephoneNumber	->	Phone Number	Remove
department	->	department	Remove
	->	localityName	Remove

For more information, see “Directory synchronization” in *Administering Avaya Aura® System Manager*.

This requirement is not applicable if you use Avaya Aura® Device Services in an environment without Avaya Aura®.

- Ensure that the mapping for the Department and City attributes is configured on each Avaya Aura® Device Services LDAP directory server. For example:

Modify LDAP Attribute Mappings

Application Field Name	Directory Field Name
City	l
Department	department

For more information, see [Modifying enterprise directory attribute mappings](#) on page 199.

Procedure

1. On the Avaya Aura® Device Services web administration portal, go to **Client Administration > Enhanced Search Configuration**.
2. In the **Department** field, 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 department 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**.

Certificate management

You can use the Avaya Aura® Device Services web administration portal to view and manage certificates. For more information, see the sections under [Certificate management](#) on page 225.

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.

Related links

[Avaya Workplace Client cannot connect to Avaya Aura Device Services](#) on page 426

[Avaya Workplace Client cannot connect to Avaya Aura Device Services when the secure connection is enabled](#) on page 427

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**.

Avaya Aura® Device Services 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

Name	Description
REST	Specifies certificate processing options for REST requests. 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 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

Name	Description
	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.

Integration with Avaya Workspaces for Avaya Oceana®

Avaya Workspaces is a browser-based application with which contact center agents can handle inbound customer operations. Avaya Workspaces uses Avaya Aura® Device Services for certain functionality. For example, the Avaya Workspaces address book uses Avaya Aura® Device Services to search for enterprise directory contacts. For information about integrating Avaya Aura® Device Services with Avaya Workspaces, see “Configuration for Avaya Workspaces” in *Administering Avaya Oceana®*.

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

1. Log in to the Avaya Aura® Device Services web administration portal with the Security administrator role.
2. Navigate to **Security Settings > Authorization**.
3. Click **Choose File** and select the .PEM file that you exported from the Avaya Breeze® platform node.
4. Click **Save**.

Dynamic Configuration service management

With the Dynamic Configuration service, Avaya Aura® Device Services can dynamically retrieve and deploy the device configuration settings to Avaya Workplace Client. For more information about the Dynamic Configuration service, see the sections under [Administration of the Dynamic Configuration service](#) on page 265.

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, 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.

*** Note:**

Avaya Aura® Device Services deployed in an environment without Avaya Aura® supports the first method only. Other methods are not supported.

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, Avaya Aura® Device Services 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.

Dynamic Configuration parameter value		Value Avaya Aura® Device Services provides to clients	
ESM_MULTISITE_ENABLED	AUTO_AMM_LOOKUP_ENABLED	ESMSRVR	ESMPORT
1	Not published. Derived value is 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.
0	Not published. Derived value is 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.
Not published. Derived value is 1	Not published. Derived value is 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	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.

Dynamic Configuration parameter value		Value Avaya Aura® Device Services provides to clients	
ESM_MULTISITE_ENABLED	AUTO_AMM_LOOKUP_ENABLED	ESMSRVR	ESMPORT
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.

Messaging server address discovery management in deployments without Avaya Aura®

When deployed in an environment without Avaya Aura®, Avaya Aura® Device Services does not interact with System Manager. Therefore, Avaya Aura® Device Services cannot obtain the messaging server FQDN and port values directly from System Manager or by performing the DNS SRV service lookup. To provide clients with the Presence Services or Avaya Multimedia Messaging server FQDN and port values, you must manually publish the ESMSRVR and ESMPORT parameters respectively using the Dynamic Configuration service.

LDAP server management

You must configure the enterprise LDAP server to authenticate the users and administrators of Avaya Aura® Device Services. The LDAP Configuration screen on the Avaya Aura® Device Services web administration portal displays the enterprise LDAP server that you configured during deployment.

You cannot perform all LDAP server management tasks with the configuration utility. Use the Avaya Aura® Device Services web administration portal to do the following:

- Configure multiple LDAP directories.
- Specify an order in which Avaya Aura® Device Services accesses LDAP directories.
- Select which LDAP directories are used for authentication.

- Configure multiple base context Distinguished Names (DNs).
- Set up LDAP synchronization.
- Configure attribute mappings.

For information about LDAP server management, see the sections under [LDAP server management](#) on page 183.

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.

Related links

[Configuring the SameSite cookie attribute](#) on page 321

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**.

Avaya Aura® Device Services displays the Cross-Origin Resource Sharing for Service interface page.

2. Select the **Enable Cross-Origin Resource Sharing** check box.

Avaya Aura® Device Services 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**.

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

For service interface, Avaya Aura® Device Services 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**.

Avaya Aura® Device Services displays the Cross-Origin Resource Sharing for Admin interface page.

2. Select the **Enable Cross-Origin Resource Sharing** check box.

Avaya Aura® Device Services 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**.

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

Avaya Aura® Device Services 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 Workplace Client desktop applications. You can upload and download of the client installer and edit or delete appcast items. For more information about the Web Deployment service, see the sections under [Web Deployment service management](#) on page 239.

Scheduling a Cassandra database repair

About this task

Avaya Aura® Device Services repairs the Cassandra database weekly to ensure that the information in the database is consistent throughout the nodes. You can select a day of the week when Avaya Aura® Device Services repairs the database or disable the repair process. By default, Avaya Aura® Device Services performs the repair process on Sundays.

Important:

The repair process might impact the Avaya Aura® Device Services performance. Therefore, Avaya recommends that you select the least busy day of the week for your enterprise.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **System Parameters > Parameter Configuration**.
2. In **NODETOOL_REPAIR_MANAGEMENT**, choose one of the following to select when Avaya Aura® Device Services performs the Cassandra database repair:
 - To change the default day of the week for the repair process, select the appropriate day of the week.
 - To disable the repair process, select **None**.
3. Click **Save**.

Related links

[Cassandra clustering configuration on Avaya Aura Device Services](#) on page 298

Chapter 4: Avaya Aura® Device Services Single Sign-On management

Single Sign-On (SSO) is an authorization flow that enables users to authenticate using a combination of enterprise credentials and other factors that the enterprise has chosen, such as multi-factor authentication. As of Release 8.0, you can configure Avaya Aura® Device Services to support SAML v2.0 and OAuth2 SSO, so that your enterprise users can log in to Avaya Workplace Client using their enterprise credentials. As of Release 10.1.1.2, you can configure Avaya Aura® Device Services to support Workspaces SSO, so that Agents can log in to Avaya Workspaces using their enterprise credentials and use AADS search APIs.

Before configuring SSO, ensure that you:

- Understand core SSO concepts.
- Gather information required for configuring SSO.

Related links

[Prerequisites for SSO configuration](#) on page 52

[Checklist for SSO authentication configuration](#) on page 55

[Checklist for configuring Microsoft Azure Active Directory integration using SAML v2.0](#) on page 58

[Checklist for configuring Ping Identity integration using SAML v2.0](#) on page 70

[Checklist for configuring OKTA integration using SAML v2.0](#) on page 76

[Checklist for configuring AD FS integration using SAML v2.0](#) on page 86

[Checklist for configuring OneLogin integration using SAML v2.0](#) on page 90

[Checklist for configuring IBM SVA integration using SAML v2.0](#) on page 95

[Checklist for configuring Duo integration using SAML v2.0](#) on page 102

[Checklist for configuring Imprivata integration using SAML v2.0](#) on page 106

SAML v2.0 and OAuth2 SSO overview

Avaya Aura® Device Services SSO involves the following key components:

- Avaya Aura® Device Services
- Keycloak
- External third-party identity provider

Avaya Aura® Device Services

Avaya Aura® Device Services implements an SSO authorization code flow for Avaya Workplace Client. Avaya Aura® Device Services initiates the SSO flow, but Avaya Aura® Device Services itself is not an identity provider. Therefore, Avaya Aura® Device Services relies on an embedded third-party component called Keycloak for token management and brokering to an external third-party identity provider.

Keycloak

Keycloak is a third-party open source component that implements a fully functional identity provider. Keycloak also supports federation and brokering to external third-party identity providers. Avaya Aura® Device Services supports the following Keycloak configurations:

- Direct integration with an enterprise directory.
- Brokering to an external third-party identity provider. Typically, this is your enterprise's identity provider.

For more information about Keycloak, see [Keycloak documentation](#).

External third-party identity provider

An identity provider manages identification information and authenticates users.

When Keycloak is configured to broker to an external identity provider, the Avaya Workplace Client user is redirected to the identity provider's Login page. The user logs in directly with the identity provider, so the user's credentials are only exchanged with the identity provider and are never passed through Avaya Aura® Device Services. The following are additional benefits of brokering:

- The Avaya Workplace Client user logs in using a familiar Login screen, which is used by all other SSO-enabled applications.
- The identity provider can implement additional authentication requirements, such as multi-factor authentication.

Avaya Aura® Device Services supports the following identity providers:

- CA SiteMender (SAML v2.0)
- Duo (SAML v2.0)
- IBM Security Verify Access (SAML v2.0)
- Imprivata (SAML v2.0)
- Microsoft Active Directory Federation Services (SAML v2.0)
- Microsoft Azure Active Directory (Azure AD, SAML v2.0)
- Microsoft Office 365 (OAuth2)
- OKTA (SAML v2.0)
- OneLogin (SAML v2.0)
- Ping Identity (SAML v2.0)
- Shibboleth (SAML v2.0)

Authentication flows

Request flow

When SSO is enabled on Avaya Aura® Device Services, the following occurs:

1. The client's authentication request is forwarded to the embedded Keycloak service.
2. Keycloak forwards this request to the third-party identity provider, which prompts the Avaya Workplace Client user to log in.

The following diagram illustrates this flow:

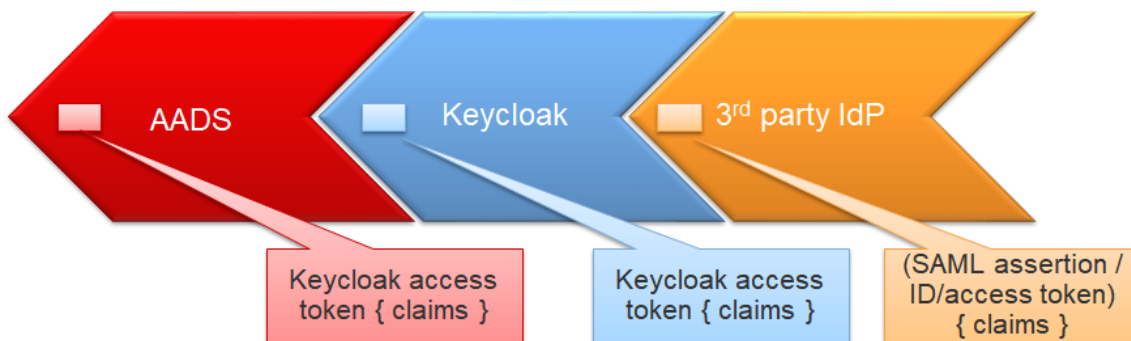


The third-party identity provider authenticates the Avaya Workplace Client user login credentials and notifies Keycloak whether the login was successful. Avaya Aura® Device Services only receives an authentication token and returns it to the client.

Response flow

The third-party identity provider passes information about the authenticated user to Keycloak using a SAML assertion or the ID or access token. The exact method depends on how Keycloak is integrated with the identity provider.

The following diagram illustrates a response flow:



The SAML assertion or the ID token contains user authentication information, such as the first name, last name or email address. The identity provider determines which information the SAML assertion or token contain. In most cases, the identity provider takes this information from an enterprise directory source.

* Note:

The SAML assertion or the ID token can contain custom attributes, such as “memberOf”, which contains the LDAP group name that Avaya Aura® Device Services associates with the user role.

For information about configuring a third-party identity provider to include custom attributes to SAML assertions or ID tokens, see documentation for the specific identity provider.

Attribute mapping between Keycloak and a third-party identity provider

A third-party identity provider sends an authentication response to Keycloak. This response contains user attributes, such as first name, last name, phone number, or email address. To send these authentication data to Avaya Workplace Client in an access token, Keycloak maps the received user attributes to the attributes of the access token. You can use the Identity Provider Mapper in Keycloak to map identity provider attributes to Keycloak attributes.

The following is an Identity Provider Mapper screen for a SAML v2.0 identity provider:

The **Attribute Name** or **Friendly Name** is the name of the attribute that Keycloak receives from the third-party provider. Keycloak uses an attribute defined in **User Attribute Name** to pass the value received from the identity provider to Avaya Workplace Client in access tokens.

For some attributes, direct mapping is not enough. Instead, you must map the attribute value received from the third-party provider and then transform it into a different value. The most common example is transforming a group value into a role.

In the following example, the identity provider releases the “memberOf” attribute with the userGroup value.



First, Keycloak uses the Attribute Importer mapper to map this attribute to an attribute with the same name, “memberOf”.

memberOf

ID

da1c4898-2eb5-47c4-9a1b-d6499f2577de

Name *

memberOf

Mapper Type

Attribute Importer

Attribute Name

memberOf

Friendly Name

User Attribute Name

memberOf

Save

Cancel

Then Keycloak transforms this attribute into a role using the Role Mapper. The value of the “memberOf” attribute is mapped to the role, and Keycloak sends this role to Avaya Workplace Client. The following image shows the Identity Mapper configuration for this transformation:

Settings

Mappers

Export

Search...

Create

Name	Category	Type
mail	Attribute Importer	Attribute Importer
user	Role Mapper	SAML Attribute to Role
GivenName	Attribute Importer	Attribute Importer
ENV	Attribute Importer	Attribute Importer
admin	Role Mapper	SAML Attribute to Role
sn	Attribute Importer	Attribute Importer
sAMAccountName	Attribute Importer	Attribute Importer
memberOf	Attribute Importer	Attribute Importer

Token authentication realm

Avaya Aura® Device Services generates SSO access and refresh tokens, which are tied to a realm named “SolutionRealm” by default. Tokens that are received from Avaya Aura® Device Services can be used to access other solution elements that support the same authentication realm, such as Avaya Aura® Web Gateway and Presence Services.

Before enabling support for these tokens on other solution elements, ensure that:

- You imported the public key from the Avaya Aura® Device Services Client ID Mapping into other solution elements.
- You configured all solution elements that use Avaya Aura® Device Services for the “SolutionRealm”.

For more information, see documentation about client mapping configuration for the corresponding solution element.

Access and refresh token expiry times

At the end of the SSO with SAML v2.0 redirect flow, Avaya Aura® Device Services returns an access and refresh token pair to Avaya Workplace Client, which uses the access token to access services on Avaya Aura® Device Services, such as contact operations or directory search. The same access token can also be used in the Unified Communication solution to access services provided by Avaya Aura® Web Gateway and Presence Services. Therefore, access tokens are as important as user name and password details.

All tokens have a configured expiry time. After the token expires, it cannot be used to access Avaya Aura® Device Services, Presence Services, or Avaya Aura® Web Gateway. For optimal security, it is essential to set a finite lifetime for access tokens.

However, if the access token lifetime is too short, then Avaya Workplace Client will prompt the user to reauthenticate, which might affect user experience. To avoid that, the associated refresh token is provided to Avaya Workplace Client so that it can get a new access token without prompting the user to log in again. When the access token is refreshed using the refresh token, a new refresh token is provided and both the access and refresh tokens have their expiry times reset. Refresh tokens also have the expiry time, which is usually longer than the expiry time for access tokens.

You can use the following main settings on the Avaya Aura® Device Services Keycloak service to configure the expiration time of access and refresh tokens:

Setting	Description	Recommendations
Access Token Lifespan	Sets the expiry time for access tokens. If the access token is expired, the refresh token is used to get a new access token without prompting the Avaya Workplace Client user to re-authenticate.	Less than 1 hour.
SSO Session Idle	Sets the expiry time for refresh tokens. If the refresh token is not used by the expiry time, then the Avaya Workplace Client user needs to log in again to get new access and refresh tokens.	Several hours.

Setting	Description	Recommendations
SSO Session Max	Sets the overall maximum time period for refresh tokens. During this time, refresh tokens can be used to obtain new access tokens. If no server or network errors occur, Avaya Workplace Client will not have to log in again until the SSO Session Max time elapses.	The time period, which is defined by your password expiration policy. For example, if your set up user passwords to expire every 180 days, then set SSO Session Max to a value that is less or equal to 180 days.  Note: Password expiration dates might be different for most users, therefore you can set SSO Session Max to a half of the password expiration period to ensure that users are required to re-authenticate with their new passwords.

For information about other parameters, see [Keycloak documentation](#).

 Important:

When configuring expiry times for refresh tokens, you must consider the following:

- The shorter the token lifetime, the more additional network traffic is generated.
- Very short token lifetimes causes Avaya Workplace Client to contact Avaya Aura® Device Services more often to refresh access tokens. On mobile clients, this might decrease the battery life.

Related links

[Configuring access and refresh token expiry times](#) on page 149

The simultaneous use of multiple identity providers

You can configure multiple identity providers on Keycloak, and the same enterprise user can have an account on each of these identity providers. Prior to Release 10.1.0, however, the user could select and use only one of the configured identity providers. Starting from Release 10.1.0, Keycloak supports the simultaneous use of multiple identity providers. Users have an option to link their identity provider accounts, so that the user can choose which identity provider to use each time they log in to their clients. The account linking procedure is performed only once when the user logs in to a client using a new identity provider.

 Note:

- Keycloak considers user accounts registered on different identity providers as belonging to the same user if these accounts use the same email address.
- For security reasons, Avaya Aura® Device Services does not automatically link user accounts registered on different identity providers.

To disable the use of an identity provider, delete its configuration from Keycloak. If users of that identity provider have accounts on other identity providers, they still can use the authentication service.

The account linking functionality is enabled by default. If required, you can configure the default account linking options in your realm on Keycloak at **Authentication > Flow > First Broker Login**. For more information about the available configuration options, see “First Login Flow” in [Server Administration Guide](#).

Identity provider account linking flow

The account linking flow looks as follows:

1. A user logs in to a client using an identity provider.
2. The user re-logs in or logs in to another device using another identity provider.
3. Keycloak notifies the user that the user account already exists.
4. The user selects the **Add to existing account** option on the Login screen.
5. Keycloak prompts the user to select an identity provider.
6. User selects an identity provider and enters authentication data.
7. Keycloak links the user accounts.

Prerequisites

To allow enterprise users to use multiple identity providers, you must:

- Disable the default identity provider, if configured. When the default identity provider is used, Keycloak automatically logs the user in to the client. Therefore, the user cannot select an identity provider when logging in to their client.
- Ensure that the **NameID Policy Format** parameter is set to **Email** on Keycloak for the identity provider. For more information about configuring identity provider settings on Keycloak, see the “Avaya Aura® Device Services integration” section for an appropriate identity provider.

Device Authorization Flow

The Device Authorization Flow, which is also called the device flow, enables users to use SSO on phones with limited input capabilities, such as J1xx phones. In this flow, the user provides SSO credentials for their phone on another device, such as a smartphone.

Avaya Aura® Device Services currently supports only the Avaya IAM identity provider for the device flow.

Avaya Aura® Device Services does not use the embedded Keycloak service in the device flow. Therefore, you do not need to configure Keycloak on Avaya Aura® Device Services. On Avaya Aura® Device Services, you need to configure settings that enable phones to interact with Avaya IAM, such as the URL to discover authentication resources or the client secret. For information about obtaining required data and configuring SSO settings on Avaya IAM, contact Avaya IAM support.

To contact Avaya IAM support:

- Submit support request to Avaya IAM (SSO) to integrate with Enterprise IDP.

- Upload your Identity Provider (IdP) metadata file using the following link:

<https://wwwcms.avaya.com/customercare/en/home/?modal=show&function=1397208961931&category=1399860014782&mode=direct>

For more information about prerequisites for the device flow configuration on Avaya Aura® Device Services, see [Prerequisites for Device Authorization Flow configuration](#) on page 54.

Limitations and considerations

- Although the device flow does not require the embedded Keycloak service, you still must enable support for SSO when installing or upgrading Avaya Aura® Device Services.
- Do not use the device flow for clients that support the Keycloak authorization flow, such as Avaya Workplace Client, Avaya Meeting Scheduler Outlook Add-in, Avaya Meetings Server Unified Portal, or Avaya Agent for Desktop.
- You cannot verify that the device flow is configured successfully using the integration test feature on the Avaya Aura® Device Services administration portal.

Related links

[Device Authorization flow configuration](#) on page 115

Prerequisites for SSO configuration

Each SSO protocol Avaya Aura® Device Services supports, that is SAML v2.0 and OAuth2 SSO, Device Authorization Flow, and Workspaces SSO, have different set of prerequisites to fulfill. Read the prerequisites corresponding to the SSO flow you are implementing before configuring Avaya Aura® Device Services.

Important:

You can only enable OAuth when you are installing or upgrading Avaya Aura® Device Services. You cannot enable OAuth at a later point.

Prerequisites for SAML v2.0 and OAuth2 SSO configuration

Before configuring SSO authentication on Avaya Aura® Device Services, gather the following information and configure an SSO application on the identity provider that you are planning to use:

SAML v2.0

- In a cluster deployment, if Avaya Aura® Device Services nodes are located in multiple data centers, ensure that port 7600 is open in the data centers for subnets where cluster nodes are deployed.
- Determine the attribute names that the identity provider sends in SAML responses for the following:
 - First name
 - Last name
 - Email address

- Group/Role indicator
- Configure the NameID format. Avaya Aura® Device Services uses the emailAddress format for NameID.
- Ensure that the identity provider supports the Service Provider-initiated (SP-initiated) flow and the SP-initiated flow is enabled and configured on the identity provider.
- Configure an SSO application on the third-party identity provider's side.
- Obtain the SAML v2.0 identity provider's IDPSSODescriptor metadata file.

You can obtain this file from the third-party identity provider.

You must import this metadata file into Keycloak when enabling SSO authentication support on Avaya Aura® Device Services or after Avaya Aura® Device Services is installed.

- Obtain the SPSSODescriptor metadata file.

You can obtain this file from the following URL after the identity provider is added to Keycloak:

```
https://<AADS_FQDN>:<AADS_PORT>/auth/realms/SolutionRealm/broker/
<SAML_V2_PROVIDER_NAME>/endpoint/descriptor
```

For example, if the Avaya Aura® Device Services front-end FQDN is aads.company.com, the AADS front-end port is the default port 443, and you created on SAML v2.0 identity provider on Keycloak with the name mySAMLProvider, then the URL for retrieving the SPSSODescriptor file is:

```
https://aads.company.com/auth/realms/SolutionRealm/broker/
mySAMLProvider/endpoint/descriptor
```

You can also obtain this file from the Keycloak administration portal.

Important:

If you download the SPSSODescriptor metadata file from the Keycloak administration portal, you must replace port 8445 with the Avaya Aura® Device Services front-end port in the following entries in the metadata file:

- <AADS_FQDN>:8445/auth/realms/SolutionRealm
- <AADS_FQDN>:8445/auth/realms/SolutionRealm/broker/<IDP_ALIAS>/endpoint

In these entries, AADS_FQDN is the Avaya Aura® Device Services FQDN and IDP_ALIAS is the identity provider alias.

The default front-end port is 443.

OAuth2

Currently, Avaya Aura® Device Services only supports the Office 365 OAuth2 identity provider.

- Determine the attribute names that the identity provider sends in OAuth2 token responses for the following:
 - First Name
 - Last Name
 - Email Address

- Client ID
- Client Secret
- Add and configure an application for SSO purposes on the Microsoft Azure portal.

Prerequisites for Device Authorization Flow configuration

Before configuring SSO authentication on Avaya Aura® Device Services, do the following:

- Obtain the following data from the Avaya IAM identity provider:
 - The Avaya IAM root CA certificate.
 - The Discovery URL address and optionally, proxy server hostnames.

You require proxy server hostnames only if the hostname of the Discovery URL is not accessible from Avaya Aura® Device Services.

- The client secret and client name configured on Avaya IAM for your organization.

Note:

The client name is mandatory and must start with "aads-" followed by a text or character. Also, configure the same client name in IAM.

Allow any combination of letters, numbers, or other characters after that.

For example:

aads-client

aads-client123

- Obtain the client ID for the phone series, such as J1XX, to configure the Device Authorization Flow.

Phone models of the same phone series have the same client ID. For example, all J1XX phones have client ID aoc-j100-cli.

- Add the Avaya IAM root CA certificate to the Avaya Aura® Device Services truststore.
- Ensure that the Discovery URL or proxy server hostname is accessible from Avaya Aura® Device Services.

To contact Avaya IAM support:

- Submit support request to Avaya IAM (SSO) to integrate with Enterprise IDP.
- Upload your Identity Provider (IdP) metadata file using the following link:

<https://wwwcms.avaya.com/customer/en/home/?modal=show&function=1397208961931&category=1399860014782&mode=direct>

Prerequisites for Workspaces SSO configuration

Avaya Aura® Device Services requires the following parameters for IAM configuration:

- Client ID, which can be any unique identifier configured for this client.
- Client Name, which is the name of the client configured on the IAM service.

For example, `workspaces`.

- OIDC URL for IAM service, which is the discovery URL of the IAM service.

If the hostname of the OIDC URL is not accessible from Avaya Aura® Device Services, use the proxy server hostnames instead.

Ensure that the OIDC URL or proxy server hostname is accessible from Avaya Aura® Device Services.

 Important:

Workspaces SSO integration does not require IAM client credentials. Therefore, you must type **NA** in the **Client Secret** field when creating a client mapping.

Related links

[Workspaces SSO Flow configuration](#) on page 118

Checklist for SSO authentication configuration

The following checklist lists the SSO configuration tasks that you can perform using the Keycloak web administration portal. Some tasks are mandatory and others are only relevant if you did not configure Keycloak using the configuration utility.

This checklist applies to Shibboleth and SiteMinder identity providers. If you use other identity providers, see the following checklists:

- If you use Duo as an identity provider, see configuration checklists in [Checklist for configuring Duo integration using SAML v2.0](#) on page 102.
- If you use IBM Security Verify Access as an identity provider, see configuration checklists in [Checklist for configuring IBM SVA integration using SAML v2.0](#) on page 95.
- If you use Imprivata as an identity provider, see configuration checklists in [Checklist for configuring Imprivata integration using SAML v2.0](#) on page 106.
- If you use Microsoft AD FS as an identity provider, see configuration checklists in [Checklist for configuring AD FS integration using SAML v2.0](#) on page 86.
- If you use Microsoft Azure Active Directory (Azure AD) as an identity provider, see configuration checklists in [Checklist for configuring Microsoft Azure Active Directory integration using SAML v2.0](#) on page 58.
- If you use Microsoft Office 365 as an identity provider, see configuration checklists in [Checklist for configuring Office 365 integration using OAuth2](#) on page 64.
- If you use OKTA as an identity provider, see configuration checklists in [Checklist for configuring OKTA integration using SAML v2.0](#) on page 76.
- If you use OneLogin as an identity provider, see configuration checklists in [Checklist for configuring OneLogin integration using SAML v2.0](#) on page 90.
- If you use Ping Identity as an identity provider, see configuration checklists in [Checklist for configuring Ping Identity integration using SAML v2.0](#) on page 70.

No.	Task	Notes	✓
1	Determine which identity provider you are using.		
2	Ensure that you gathered all required information and configured an SSO application on your third-party identity provider.	See Prerequisites for SSO configuration on page 52. Before configuring authentication settings on Keycloak, you must configure an SSO application on the identity provider's side and obtain the IDPSSODescriptor file from the identity provider. For more information, contact your identity provider.	
3	Ensure that the realm is created.	The realm, which is called SolutionRealm by default, is typically created automatically when you configure Keycloak in the Avaya Aura® Device Services configuration utility. Verify this when you log in to the Keycloak web administration portal. If the realm was not created automatically, contact Avaya support. Ensure that the realm value is properly provisioned to Avaya Workplace Client soft phones and other UC servers configured to use the Authorization service. For more information, see Authorization realm configuration on UC servers and Avaya Workplace Client on page 123.	
4	Configure Keycloak settings using the Avaya Aura® Device Services configuration utility.	See Configuring Keycloak settings on page 124.	
5	Obtain the client secret.	See Obtaining the client secret on page 126. The client secret is required to enable communication between Avaya Aura® Device Services and Keycloak.	
6	Create client mapping.	See Creating client mapping on page 126. If you need to regenerate the client secret, see Regenerating the Keycloak client secret on page 129.	
7	Optional: Import a third-party identity provider.	See Importing a third-party identity provider on page 131.	

No.	Task	Notes	✓
		This task is only required if you did not import the identity provider using the Avaya Aura® Device Services configuration utility. ! Important: You can use the configuration utility to upload an entity descriptor file for the Shibboleth identity provider only. For other identity providers, you must upload the file using the Keycloak web portal. If the third-party identity provider uses a certificate signed by a private CA, you must import the CA certificate chain for the identity provider to the default Java truststore. For more information, see Importing third-party identity provider private CA certificates on page 130.	
8	Optional: Select the default identity provider to use for authorization.	See Selecting the default identity provider on page 132. This task is only required if you did not import an identity provider using the Avaya Aura® Device Services configuration utility. Do not perform this task if you want to allow the simultaneous use of multiple identity providers to your enterprise users.	
9	Optional: Modify the attribute mapping between the third-party identity provider and Keycloak.	Perform this task if the identity provider uses different attribute names than the ones in the default mapping. See Modifying the attribute mapping between the third-party identity provider and Keycloak on page 133.	
10	Configure the LDAP UID mapping	See Configuring the LDAP UID mapping on page 144.	
11	Test the integration with the identity provider.	See Testing the integration with an identity provider from the Google Chrome web browser on page 146.	
12	Configure expiry time for access and refresh tokens.	See Configuring access and refresh token expiry times on page 149.	

Related links

[Prerequisites for SAML v2.0 and OAuth2 SSO configuration](#) on page 52

Avaya Aura Device Services integration with Microsoft Azure Active Directory

Checklist for configuring Microsoft Azure Active Directory integration using SAML v2.0

The following checklist lists the configuration tasks that you perform on the Microsoft Azure web portal and the Keycloak web administration portal to set up integration with Microsoft Azure Active Directory (Azure AD) using SAML v2.0.

No.	Task	Notes	✓
1	Ensure that you gathered all required information for configuring integration.	See Prerequisites for SSO configuration on page 52.	
2	Create and configure an application for SSO on Microsoft Azure.	See Creating a new application on page 59.	
3	Configure user and administrator groups on Microsoft Azure.	See Configuring user and administrator groups on page 61 and Adding users to groups on page 61.	
4	Obtain the user and administrator group IDs.	See Obtaining the group ID on page 62.	
5	Select Microsoft Azure Active Directory users and groups that can use SSO capabilities.	See Assigning users and groups to the SSO application on Microsoft Azure on page 62.	
6	Configure Keycloak settings using the Avaya Aura® Device Services configuration utility.	See Configuring Keycloak settings on page 124.	
7	Configure a Azure AD SAML v2.0 identity provider on Keycloak.	See Configuring an Azure AD SAML v2.0 identity provider on Keycloak on page 63.	
8	Configure attribute mapping between the Office 365 SAML v2.0 identity provider and Keycloak.	See Modifying the attribute mapping between the third-party identity provider and Keycloak on page 133. For information about mappers that you must configure on Keycloak, see Attribute mapping parameters for Microsoft Azure SAML v2.0 identity provider on page 136.	
9	Obtain the client secret.	See Obtaining the client secret on page 126. The client secret is required to enable communication between Avaya Aura® Device Services and Keycloak.	

No.	Task	Notes	✓
10	Create a client mapping.	See Creating client mapping on page 126. If you need to regenerate the client secret, see Regenerating the Keycloak client secret on page 129.	
11	Configure the LDAP UID mapping.	See Configuring the LDAP UID mapping on page 144.	
12	Select the identity provider to use for authorization.	See Selecting the default identity provider on page 132. Do not perform this task if you want to allow the simultaneous use of multiple identity providers to your enterprise users.	
13	Test the integration with Azure AD.	See Testing the integration with the identity provider from the web administration portal on page 147.	
14	Configure expiry time for access and refresh tokens.	See Configuring access and refresh token expiry times on page 149.	

Creating a new application

About this task

Use this procedure to configure a new application for SSO on the Microsoft Azure portal.

When configuring the application, you obtain an identity provider alias and configuration file. You will need this data later when configuring an Azure AD identity provider on Keycloak.

Before you begin

Ensure that you:

- Have an active Microsoft Azure subscription.
- Have an administrative account with the Global Administrator role.

Procedure

1. Log in to <https://portal.azure.com> as an administrator.
2. Navigate to **Azure Active Directory > Enterprise Applications > All applications**.
3. On the All applications page, click **New application**.
4. Click **Create your own application**.
5. In **Name**, type a name of your choice for the application.
6. In **What are you looking to do with your application?**, select **Integrate any other application you don't find in the gallery**.

7. Click **Create**.
8. Navigate to the **All applications** page and click the application that you have just created.
9. On the Overview page, in the Getting Started area, click **Set up single sign-on**.
10. In the Select a single sing-on method area, select **SAML**.
Microsoft Azure displays the Single Sign-On with SAML — Preview page.
11. On the Set up Single Sign-On with SAML page, in the Basic SAML Configuration area, click **Edit**.
12. On the Basic SAML configuration page, configure the following settings:
 - a. In **Identifier (Entity ID)**, type `https://<AADS FQDN>/auth/realms/SolutionRealm`.
In this string, <AADS FQDN> is the Avaya Aura® Device Services front-end FQDN.
 - b. In **Reply URL (Assertion Consumer Service URL)**, type `https://<AADS FQDN>/auth/realms/SolutionRealm/broker/<IDP alias>/endpoint`.
In this string, <IDP alias> is an identity provider alias of your choice. For example, AzureSAML.
 - c. Leave default values for other fields.
 - d. Click **Save**.
13. Remember the identity provider alias that you used in the previous step.
You will use this alias when creating an Azure AD SAML provider on Keycloak.
14. On the Set up Single Sign-On with SAML page, in the User Attributes and Claims area, click **Edit**.
15. On the User Attributes & Claims page, click **Add a group claim** and then configure the following settings:
 - a. In **Which groups client used by Azure AD to populate SAML tokens**, select **All groups**.
 - b. In **Source attribute**, select **Group ID**.
 - c. Leave default values for other fields.
 - d. Click **Save**.
16. In the SAML Signing certificate area, click **Download** next to Federation Metadata XML to download an XML file with federation metadata.
You will use this XML configuration file when creating an Azure AD SAML provider on Keycloak.
17. Click **Save**.

Configuring user and administrator groups

About this task

You must create the following two groups, which IDs you will use to configure attribute mapping between Keycloak and Azure AD:

- User group.
- Administrator group, which is used for administration purposes.

Every Azure AD user who requires SSO capabilities must belong to either of these groups.

Procedure

Repeat the following steps for each group:

1. Log in to the Microsoft Azure portal as a Global Administrator.
2. Navigate to **Azure Active Directory > Groups**.
3. Click **New group**.
4. In **Group type**, select **Security**.
5. In **Group name**, type a name of your choice for the group.
For example, `USER` for the user group and `ADMIN` for the administrator group.
6. In **Group description**, provide a description for the group.
7. In **Owners**, click **No owners selected**, select an appropriate owner for the group and then click **Select**.
8. In **Members**, click **No members selected**, select users that you want to add to the group and then click **Select**.
9. Click **Create**.

Adding users to groups

About this task

Every Azure AD user who requires SSO capabilities must belong to one of groups which IDs are used in the attribute mapping between Azure AD and Keycloak.

About this task

Configure the required groups as described in [Configuring user and administrator groups](#) on page 61.

Procedure

1. Log in to the Microsoft Azure administration portal as a Global Administrator.
2. Navigate to **Azure Active Directory > Groups**.
3. Select an appropriate group.
4. On the Group page, click **Members**.

5. Click **Add members**.
6. Select users that you want to add to the group.
7. Click **Select**.

Obtaining the group ID

About this task

User and administration group IDs are must to configure attribute mapping between Azure AD and Keycloak.

Before you begin

Configure the groups described in [Configuring user and administrator groups](#) on page 61.

Procedure

1. Log in to the Microsoft Azure administration portal as a Global Administrator.
2. Navigate to **Azure Active Directory > Groups**.
3. Select a group.
4. Copy the value of the **Object Id** field.
5. Repeat steps 2 to 4 to obtain the ID of another group.

Next steps

Configure attribute mapping between Azure AD and Keycloak.

Assigning users and groups to the SSO application on Microsoft Azure

About this task

To enable SSO capabilities to an Azure AD user or a group, assign this user or group to your application for SSO.

Procedure

1. Log in to the Microsoft Azure administration portal as a Global Administrator.
2. Navigate to **Azure Active Directory > Enterprise Applications**, and select your application for SSO.
3. In the left navigation pane, click **Users and groups**.
4. In the Getting Started area, click **Assign users and groups**.

Microsoft Azure displays the list of users and groups in the Active Directory.

5. On the Users and groups page, click **Add user/group**.
6. On the Add Assignment page, click **Users and groups**.
7. Select one or more users or groups you want to assign to the application.

8. Click **Select** and click **Assign**.

Configuring an Azure AD SAML v2.0 identity provider on Keycloak

About this task

To use Azure AD SSO capabilities and authenticate users, configure a SAML v2.0 identity provider on Keycloak.

Before you begin

Configure an application for SSO on Microsoft Azure and obtain a configuration metadata file in XML format. For more information on configuring an application, see [Creating a new application](#) on page 59.

Procedure

1. Log in to the Keycloak web administration interface.
2. By default the administration interface displays **Master**. From the dropdown list, select **Solution Realm > Identity Provider**.
3. Click **Add provider** and select **SAML v2.0**.
4. In **Alias**, type the name that you used when configuring a SAML application on Microsoft Azure.

For example, `AzureSAML`.

5. Set **Use entity descriptor** to **Off**.

Note:

Setting **Use entity descriptor** to off is applicable for new users who are configuring IDP for the first time.

6. Click **Select file**, navigate to the federation metadata XML file that you downloaded from Microsoft Azure, and click **Import**.

Keycloak imports the configuration data and populates the **Single Sign-On Service URL** field.

7. In **NameID Policy Format**, select **Email**.
8. Click **Save**.

Next steps

Configure attribute mapping between Keycloak and the Azure AD identity provider.

Avaya Aura® Device Services integration with Office 365 using OAuth2

If you use Office 365 in your deployment, you can configure SSO capabilities for authentication on Avaya Workplace Client. You can use the OAuth2 integration method for authentication and authorization.

*** Note:**

The OAuth2 method might have limitations comparing to SAML v2.0. For example, integration with OAuth2 currently requires you to add the user role to all users that must authenticate using Office 365. If you want to use the SAML v2.0 authentication method in the Microsoft Azure environment, configure SSO as described in [Checklist for configuring Microsoft Azure Active Directory integration using SAML v2.0](#) on page 58.

Checklist for configuring Office 365 integration using OAuth2

The following checklist lists the configuration tasks that you perform on the Microsoft Azure web portal and the Keycloak web administration portal to set up integration with Office 365 using OAuth2.

No.	Task	Notes	✓
1	Ensure that you gathered all required information for configuring integration.	See Prerequisites for SSO configuration on page 52.	
2	Register an application for SSO purposes on Microsoft Azure.	See Registering an application for SSO purposes on page 65.	
3	Enable the application to read data from the Microsoft Azure Active Directory.	See Allowing the application to read Microsoft Azure directory data on page 66.	
4	Obtain the following application data: • Application ID • Application Client secret.	See Obtaining the application ID on page 66 and Obtaining the application client secret on page 67. You must have this data when you configure an identity provider on Keycloak.	
5	Configure an Office 365 OAuth2 identity provider on Keycloak.	See Adding an Office365 OAuth2 identity provider to Keycloak on page 67.	
6	Disable the identity provider redirector.	See Disabling the identity provider redirector on page 68.	
7	Add a hard-coded user role in Keycloak	See Adding a hard-coded user role in Keycloak on page 68.	

No.	Task	Notes	✓
8	Configure attribute mapping between the Office 365 identity provider and Keycloak.	See Modifying the attribute mapping between the third-party identity provider and Keycloak on page 133. For information about mappers that you must configure on Keycloak, see Attribute mapping parameters for Office 365 OAuth2 identity provider on page 136.	
9	Configure the LDAP UID mapping.	See Configuring the LDAP UID mapping on page 144.	
10	Test the integration with Office 365.	See Testing the integration with an identity provider from the Google Chrome web browser on page 146.	
11	Configure expiry time for access and refresh tokens.	See Configuring access and refresh token expiry times on page 149.	

Registering an application for SSO purposes

About this task

Register an application in Microsoft Azure. When configuring this application, you obtain data that are required to configure the Office 365 identity provider on Keycloak to enable your enterprise users to log in to Avaya Workplace Client with Office 365 credentials.

Before you begin

Ensure that you have an Office 365 account with privileges for creating applications.

Procedure

1. Log in to <https://portal.azure.com> as an Office 365 administrator.
2. Navigate to **Azure Active Directory > App registrations**.
Microsoft Azure displays the App registrations page.
3. At the top of the page, click **New registration**.
Microsoft Azure displays the Register an application page.
4. In **Name**, provide a name for the application.
For example, AADS.
5. In **Supported account type**, select **Accounts in any organizational directory (Any Azure AD directory — Multitenant)**.
6. In **Redirect URI**, enter `https://<AADS_FQDN>:<AADS_PORT>/auth/realms/SolutionRealm/broker/microsoft/endpoint`.

In these strings, <AADS FQDN> is the Avaya Aura® Device Services front-end FQDN. AADS PORT is the Avaya Aura® Device Services front-end port.

7. Click **Register**.

Microsoft Azure displays the Overview page for your application.

Obtaining the application ID

About this task

Use this procedure to obtain the ID for the application you registered on Microsoft Azure. Avaya Aura® Device Services uses this application ID when adding a new identity provider.

Before you begin

Register an application on Microsoft Azure as described in [Registering an application for SSO purposes](#) on page 65.

Procedure

1. On Microsoft Azure, navigate to **Azure Active Directory > App registrations**.
2. Navigate to your application.
3. On the Overview page, click the **Copy** icon next to the **Application ID** field and save it in a safe location.

Allowing the application to read Microsoft Azure directory data

About this task

You must allow the SSO application you created to read data in your organization's directory. Users must consent to having their data read or you can grant administrative consent on behalf of all users.

Before you begin

Create an application for SSO.

Procedure

1. On Microsoft Azure, from **App registration**, navigate to your SSO application.
2. To grant consent on behalf of all users in your organization's directory, do the following:
 - a. In Configured permissions, click **Grant admin consent for <your admin name here>** to grant consent on behalf of all users in your organization's directory.
 - b. In the Confirmation window, enter your administrator credentials to confirm changes.
3. In the Manage section on the left-hand side of the screen, click **API permissions**.
4. Click **Add a permission**.
5. In the Request API permission section, click **Azure Active Directory Graph**.

Microsoft Azure displays the Permission Properties window.

6. Select **Delegated permissions**.
7. In the Select permissions area, click **Directory** and select the **Directory.Read.All** check box.
8. Click **Add permissions**.
9. **(Optional)** If Microsoft Azure prompts you to enter your administrator credentials, repeat step 2.

Obtaining the application client secret

About this task

When obtaining authentication tokens, Avaya Aura® Device Services uses a client secret to authenticate with Microsoft Azure Active Directory. You will use the client secret when configuring an identity provider on Avaya Aura® Device Services Keycloak. Use this procedure to generate and obtain a client secret for your SSO application on Microsoft Azure.

Important:

You must copy and save a client secret immediately after creating it. You *cannot* see the secret again after you leave the Client secret configuration page.

Before you begin

Register an application on Microsoft Azure as described in [Registering an application for SSO purposes](#) on page 65.

Procedure

1. On Microsoft Azure, navigate to **Azure Active Directory > App registrations**.
2. Navigate to your application.
3. In the Manage area, click **Certificates & secrets**.
4. In the Client secrets area, click **New client secret**.
5. Provide a description for the client secret.
6. Select the expiration time for the client secret.
7. Click **Add**.

Microsoft Azure generates a new client secret.

8. Click **Copy** next to the client secret and save it in a safe location before leaving the page.

Adding an Office365 OAuth2 identity provider to Keycloak

About this task

To use SSO capabilities and authenticate users using Office365, you must configure the Office365 identity provider on Keycloak.

When you create an Office 365 identity provider, Keycloak automatically generates a redirect URI. Your Microsoft Azure application sends authentication tokens to this URI.

Before you begin

Obtain the application ID and client secret for the application you registered on Microsoft Azure.

Procedure

1. On the Keycloak web administration interface, navigate to **Identity Providers**.
2. Click **Add provider** and select **Microsoft**.
Keycloak displays the Add identity provider page.
3. In **Client ID**, enter the application ID you copied from your Microsoft Azure application.
4. In **Client Secret**, enter the client secret you copied from your Microsoft Azure application.
5. Click **Save** to create the identity provider.

Disabling the identity provider redirector

About this task

When you configure Office 365 integration for authentication purposes using OAuth2, the identity provider redirector must be disabled on Keycloak.

Procedure

1. On the Keycloak web administration portal, in the left pane, click **Authentication**.
2. On the Flows tab, click the drop-down field and select **Browser**.
3. For **Identity Provider Redirector**, select **Disabled**.

Adding a hard-coded user role in Keycloak

About this task

Authentication tokens generated by Keycloak must contain role information to enable Avaya Workplace Client to use SSO capabilities. In Avaya Aura® Device Services deployments that do not use the Enterprise SSO capability, the user role is assigned to users of the LDAP group configured as the user role. Avaya Aura® Device Services does not restrict access to users outside the user group. Therefore, you can add a hard-coded user role to the Keycloak configuration for OAuth2 identity providers that cannot provide group membership information. In this case, Keycloak assigns this hard-coded user role to all users that successfully authenticate with the OAuth2 identity provider.

If you configured integration with Office 365 using OAuth2, you cannot use the Keycloak web administration portal to create attribute mappings from the OAuth2 token to a role. You can only use the “Hardcoded Role” mapper type.

Note:

Hardcoded Role also works for other Identity Providers (IDP) and is tested for Active Directory Federation Service (ADFS).

Procedure

1. Log in to the Keycloak web administration interface.

For more information, see [Logging in to the Keycloak web administration portal](#) on page 122.

2. On the Keycloak web administration interface, navigate to your Office 365 OAuth2 identity provider.
3. Click the **Mappers** tab.
4. Click **Create**.

Keycloak displays the Add Identity Provider Mapper page.

5. In **Name**, provide a name for the mapper.

For example: `user.groups`

6. From **Mapper Type**, select **Hardcoded Role**.
7. Click **Select Role**.

Keycloak displays the Role Selector page.

8. From the **Client Roles** drop-down list, select **aads**.
9. In the area below the **Client Roles** drop-down list, select **user**.
10. Click **Select client role**.
11. On the Add Identity Provider Mapper page, click **Save**.

Configuring identical Roles for Multiple Groups in Keycloak

Procedure

1. Log in to the Keycloak web administration interface.
For more information, see [Logging in to the Keycloak web administration portal](#) on page 122.
2. On the Keycloak web administration interface, navigate to **Solution Realm > Identity providers**.
3. In the **Identity Providers** page, click the required provider.
4. Click the **Mappers** tab.
5. Click **Add Mapper**.

Keycloak displays the Add Identity Provider Mapper page.

6. In the **Name** field, provide a name for the mapper.

For example: `aads.user`

Sync mode override field has the value **Inherit** selected by default.

7. From the **Mapper Type** drop-down menu, select **Advanced Attribute to Role**.
8. Enter the **Attributes Key** as required by the customer.

9. Use Regex expressions to combine multiple groups that assign the same role and add the **Attributes Value**.
10. Turn the **Regex Attribute Values** button **On**.
11. Click **Select Role**.
Keycloak displays the Role Selector page.
12. To filter options based on clients select **Filter by clients** from the filter drop-down list.
13. From the list of clients select the required option. For example: **aads.user**.
14. Click **Assign**.
15. On the Add Identity Provider Mapper page, click **Save**.

Avaya Aura Device Services integration with Ping Identity

Checklist for configuring Ping Identity integration using SAML v2.0

The following checklist lists the configuration tasks that you perform on the Ping Identity and Keycloak web administration portals to set up integration with Ping Identity using SAML v2.0.

No.	Task	Notes	✓
1	Ensure that you gather all required information for configuring the integration.	See Prerequisites for SSO configuration on page 52.	
2	Create and configure an application for SSO using the PingOne console.	See Creating a new SAML v2.0 application on Ping Identity on page 71.	
3	Obtain the Ping Identity configuration file.	See Obtaining the XML configuration file on page 72.	
4	Configure Keycloak settings using the Avaya Aura® Device Services configuration utility.	See Configuring Keycloak settings on page 124.	
5	Configure a Ping Identity identity provider on Keycloak.	See Configuring a Ping Identity SAML v2.0 identity provider on Keycloak on page 75.	
6	Configure user and administrator Population groups on Ping Identity.	See Configuring user and administrator Population groups on page 73.	
7	Configure attribute mapping on Ping Identity.	See Configuring attribute mapping on Ping Identity on page 74.	

No.	Task	Notes	✓
8	Configure attribute mapping between the Ping Identity SAML v2.0 identity provider and Keycloak.	See Modifying the attribute mapping between the third-party identity provider and Keycloak on page 133. For information about mappers that you must configure on Keycloak, see Attribute mapping parameters for Ping Identity SAML v2.0 identity provider on page 137.	
9	Obtain the client secret.	See Obtaining the client secret on page 126. The client secret is required to enable communication between Avaya Aura® Device Services and Keycloak.	
10	Create a client mapping.	See Creating client mapping on page 126. If you need to regenerate the client secret, see Regenerating the Keycloak client secret on page 129.	
11	Configure the LDAP UID mapping.	See Configuring the LDAP UID mapping on page 144.	
12	Select the identity provider to use for authorization.	See Selecting the default identity provider on page 132. Do not perform this task if you want to allow the simultaneous use of multiple identity providers to your enterprise users.	
13	Create users on Ping Identity.	See Creating users on Ping Identity on page 76.	
14	Test the integration with Ping Identity.	See Testing the integration with the identity provider from the web administration portal on page 147.	
15	Configure expiry time for access and refresh tokens.	See Configuring access and refresh token expiry times on page 149.	

Creating a new SAML v2.0 application on Ping Identity

About this task

Use this procedure to configure a new application for SSO on Ping Identity using the PingOne console.

When configuring the application, you obtain an identity provider alias and configuration file. You will need this data later when configuring an Ping Identity SAML v2.0 identity provider on Keycloak.

Before you begin

- Register an account on Ping Identity.
- Install the PingID application. For information, see [PingID Downloads](#).
- Install the PingOne application. For information, see [PingOne for Customers](#).

Procedure

1. Log in to the PingOne console as the administrator.
2. Navigate to **Connection > Applications**.
3. On the Applications page, click **Add Application**.
4. On the Choose Connection Type page, select **WEB APP**.
5. Select **SAML** and then click **Configure**.
6. On the Create App Profile page, in **Application Name**, type a name for your SAML 2.0 application and then click **Next**.
7. On the Configure SAML Connection page, complete the following fields:
 - a. In **ACS URLS**, enter `https://<AADS_FQDN>/auth/realms/SolutionRealm/broker/<IDP_ALIAS>/endpoint`.

In these strings, <AADS_FQDN> is the Avaya Aura® Device Services front-end FQDN. <IDP_ALIAS> is an identity provider alias of your choice. For example, PingIdentitySAML.
 - b. In **ENTITY ID**, enter `https://<AADS_FQDN>/auth/realms/SolutionRealm`.
 - c. In **ASSERTION VALIDITY DURATION**, enter 300.
 - d. Leave default values for all other fields.
8. Remember the identity provider alias that you used in the previous step.
You will use this alias later when creating a Ping Identity SAML v2.0 provider on Keycloak.
9. Skip the configuration of settings on the Attribute mappings page.
10. Click **Save**.

Next steps

Obtain the Ping Identity configuration file in XML format.

Obtaining the XML configuration file

About this task

Use this procedure to obtain an XML file with configuration metadata for the Ping Identity identity provider.

Before you begin

Configure a Ping Identity SAML application.

Procedure

1. Log in to the PingOne console as the administrator.
2. Navigate to **Connection > Applications**.
3. Select your SAML application.
4. Go to the **Configuration** tab.
5. Click **Download** and save the `metadata.xml` file on your computer.

Next steps

Configure the Ping Identity identity provider on Keycloak.

Configuring user and administrator Population groups

About this task

A population group defines a set of users on Ping Identity. You must create the following Population groups on Ping Identity:

- User group.
- Administrator group, which is used for administration purposes.

You also use these population group settings to configure attribute mapping between Ping Identity and Keycloak.

* Note:

The SSO capabilities are available to members of both these groups.

Procedure

1. Log in to the PingOne console as the administrator.
2. Navigate to **Identities > Populations**.
3. Create an administrator Population group as follows:
 - a. Click **Add Population**.
 - b. In **Name**, type a name of your choice.
For example, `Admin`.
 - c. Click **Save**.
PingOne displays information about the created group.
 - d. Remember the **Population ID** value.
You will use this value later when configuring attribute mapping on Keycloak.
4. Create a user Population group as follows:
 - a. Click **Add Population**.
 - b. In **Name**, type a name of your choice for the group.
For example, `User`.

- c. Click **Save**.

PingOne displays information about the created group.

- d. Remember the **Population ID** value.

You will use this value later when configuring attribute mapping on Keycloak.

Next steps

Add users to Ping Identity.

Configuring attribute mapping on Ping Identity

About this task

To authenticate a user, Ping Identity sends an authentication response to Keycloak containing various user attributes, such as the first name, last name, phone number, or email address. Keycloak then maps this user information to the attributes of the access token that is generated and sent back to clients. Use this procedure to specify Keycloak attribute names on Ping Identity.

Procedure

1. Log in to the PingOne console as the administrator.
2. Navigate to **Connection**.
3. Select your SAML v2.0 application.
4. Select **Attribute mapping** and then select **Edit**.
5. Configure attribute mapping as follows:

PingOne user attribute	Application attribute	Required
Username	saml_subject	Required
Population ID	Group	Required
Email Address	email	Required
Given Name	firstName	Required
Family Name	lastName	Required

The following image displays configured attribute mapping on Ping Identity:

PINGONE USER ATTRIBUTE		APPLICATION ATTRIBUTE	
 Email Address	=	 email	REQUIRED
 Family Name	=	 lastName	REQUIRED
 Given Name	=	 firstName	REQUIRED
 Population ID	=	 Group	REQUIRED
 Username	=	 saml_subject	REQUIRED

6. Click **Save**.

Configuring a Ping Identity SAML v2.0 identity provider on Keycloak

About this task

To use Ping Identity SSO capabilities and authenticate users, you must configure a SAML v2.0 identity provider on Keycloak.

Before you begin

- Configure a SAML application on Ping Identity.
- Obtain a configuration file in XML format. For more information, see [Obtaining the XML configuration file](#) on page 72.

Procedure

1. Log in to the Keycloak web administration interface.
2. Navigate to **Solution Realm > Identity Providers**.
3. Click **Add provider** and then select **SAML v2.0**.
4. In **Alias**, type the name that you used when configuring a SAML application on Ping Identity.

For example, `PingIdentitySAML`. For more information, see step [7](#) on page 72.

5. Navigate to the Import External IDP Config section.
6. Click **Select file**, navigate to the Ping Identity configuration XML file that is stored on your computer, and then click **Import**.

Keycloak imports the configuration data and populates the **Single Sign-On Service URL** field.

7. From **NameID Policy Format**, select **Email**.
8. Click **Save**.

Creating users on Ping Identity

About this task

Use this procedure to add a user who requires SSO capabilities on Ping Identity.

Procedure

1. Log in to the PingOne console as the administrator.
2. Navigate to **Identities > Users**.
3. Click **Add User**.
4. In **Given Name**, type the first name of the user.
5. In **Family Name**, type the last name of the user.
6. In **Email Address**, type the email address of the user.
7. In **Username**, type a unique identifier for the user.

You can use the user email address as a username.

8. In **Population**, select either the user group or the administrator population group that you created.

The SSO capabilities are available to members of both groups. Select the administrator population group if you want to provide the user with the administrator rights.

9. Complete other fields as required.

Avaya Aura Device Services integration with OKTA

Checklist for configuring OKTA integration using SAML v2.0

The following checklist lists the configuration tasks that you perform on the OKTA and Keycloak web administration portals to set up integration with OKTA using SAML v2.0.

No.	Task	Notes	✓
1	Ensure that you gather all required information for configuring the integration.	See Prerequisites for SSO configuration on page 52.	
2	Create and configure an application for SSO.	See Creating a new SAML v2.0 application on OKTA on page 78.	
3	Obtain the OKTA configuration file.	See Obtaining the XML configuration file on page 79.	

No.	Task	Notes	✓
4	Configure Keycloak settings using the Avaya Aura® Device Services configuration utility.	See Configuring Keycloak settings on page 124.	
5	Configure the OKTA identity provider on Keycloak.	See Configuring an OKTA SAML v2.0 identity provider on Keycloak on page 79.	
6	Configure user and administrator groups on OKTA.	See Configuring user and administrator groups on page 80.	
7	Create users on OKTA.	See Creating users on OKTA on page 81.	
8	Add users to groups on OKTA.	See Adding users to groups on page 81.	
9	Assign the user group to the SAML v2.0 application on OKTA.	See Assigning a group to an OKTA SAML application on page 82.	
10	Configure attribute mapping on OKTA.	See Configuring attribute mapping on OKTA on page 82.	
11	Configure attribute mapping between the OKTA SAML v2.0 identity provider and Keycloak.	See Modifying the attribute mapping between the third-party identity provider and Keycloak on page 133. For information about mappers that you must configure on Keycloak, see Attribute mapping parameters for OKTA SAML v2.0 identity provider on page 138.	
12	Obtain the client secret.	See Obtaining the client secret on page 126. The client secret is required to enable communication between Avaya Aura® Device Services and Keycloak.	
13	Create a client mapping.	See Creating client mapping on page 126. If you need to regenerate the client secret, see Regenerating the Keycloak client secret on page 129.	
14	Configure the LDAP UID mapping.	See Configuring the LDAP UID mapping on page 144.	
15	Select the identity provider to use for authorization.	See Selecting the default identity provider on page 132. Do not perform this task if you want to allow the simultaneous use of multiple identity providers to your enterprise users.	

No.	Task	Notes	✓
16	Test the integration with OKTA.	See Testing the integration with the identity provider from the web administration portal on page 147.	
17	Configure expiry time for access and refresh tokens.	See Configuring access and refresh token expiry times on page 149.	

Creating a new SAML v2.0 application on OKTA

About this task

Use this procedure to configure a new application for SSO on the OKTA administration portal.

When configuring the application, you obtain an identity provider alias and configuration file. You will need this data later when configuring an OKTA SAML v2.0 identity provider on Keycloak.

Before you begin

- Register an account on OKTA.
- Install the OKTA Verify application. This application is required to log in to your account as an administrator. For information, see [OKTA Verify](#).

Procedure

1. Log in to your OKTA account as an administrator.
2. Navigate to **Application**.
3. Click **Add Application**.
4. On the Add Application page, click **Create New App**.
OKTA displays the Create a New Application Integration window.
5. In the Create a New Application Integration window, do the following:
 - a. In **Platform**, select **Web**.
 - b. In **Sign on method**, select **SAML 2.0**.
6. Click **Create**.
7. On the General Settings tab, in **App name**, type a name of your choice for the application and then click **Next**.
8. On the Configure SAML tab, configure the following settings:
 - a. In **Single sign on URL**, enter `https://<AADS FQDN>/auth/realms/SolutionRealm/broker/<IPD ALIAS>/endpoint`.
In this string, <AADS FQDN> is the Avaya Aura® Device Services front-end FQDN. <IDP alias> is an identity provider alias of your choice. For example, oktaSAML.
 - b. Select the **Use this for Recipient URL and Destination URL** check box.
 - c. In **Audience URI (SIP Entity ID)**, enter `https://<AADS FQDN>/auth/realms/SolutionRealm/broker/<IPD ALIAS>/endpoint`.

In this string, <AADS_FQDN> is the Avaya Aura® Device Services front-end FQDN.
<IDP_alias> is an identity provider alias of your choice. For example, `oktaSAML`.

d. For other fields, keep default values.

9. Remember the identity provider alias that you used in the previous step.

You will use this alias later when creating an OKTA SAML v2.0 provider on Keycloak.

10. Click **Next**.

11. Click **Finish**.

Next steps

Download the IDP metadata XML file.

Obtaining the XML configuration file

About this task

Use this procedure to obtain an XML file with configuration metadata for the OKTA identity provider.

Before you begin

Configure an OKTA SAML application.

Procedure

1. Log in to the OKTA web portal as an administrator.
2. Navigate to **Application**.
3. Select your SAML application.
4. Go to the **Sign On** tab.
5. Click **Identity Provider metadata** and save the XML file with configuration metadata on your computer.

Next steps

Configure the OKTA identity provider on Keycloak.

Configuring an OKTA SAML v2.0 identity provider on Keycloak

About this task

To use OKTA SSO capabilities and authenticate users, you must configure a SAML v2.0 identity provider on Keycloak.

Before you begin

- Configure an OKTA SAML application.
- Obtain a configuration file in XML format. For more information, see [Obtaining the XML configuration file](#) on page 79.

Procedure

1. Log in to the Keycloak web administration interface.
2. Navigate to **Solution Realm > Identity Providers**.
3. Click **Add provider** and then select **SAML v2.0**.
4. In **Alias**, type the name that you used when configuring a SAML application on the OKTA web administration portal.

For example, `oktaSAML`. For more information, see step [8](#) on page 78.

5. Navigate to the Import External IDP Config section.
6. Click **Select file**, navigate to the OKTA configuration metadata XML file that is stored on your computer, and then click **Import**.

Keycloak imports the configuration data and populates the **Single Sign-On Service URL** field.

7. From **NameID Policy Format**, select **Email**.
8. Click **Save**.

Configuring user and administrator groups

About this task

A group defines a set of users on OKTA. You must create the following groups on OKTA:

- User group.
- Administrator group, which is used for administration purposes.

You also use these group settings to configure attribute mapping between OKTA and Keycloak.

Note:

The SSO capabilities are available to members of both these groups.

Procedure

1. Log in to the OKTA administration portal as the administrator.
2. Navigate to **Directory > Groups**.
3. Create an administrator group as follows:

- a. Click **Add Group**.
- b. In **Name**, type a name of your choice.

For example, `Admin`.

- c. In **Group Description**, type a description for the group.
- d. Click **Add Group**.

OKTA displays information about the created group.

- e. Remember the **Name** value.

You will use this value later when configuring attribute mapping on Keycloak.

4. Create a user group as follows:

- a. Click **Add Group**.
- b. In **Name**, type a name of your choice for the group.
For example, `User`.
- c. In **Group Description**, type a description for the group.
- d. Click **Add Group**.

OKTA displays information about the created group.

- e. Remember the **Name** value.

You will use this value later when configuring attribute mapping on Keycloak.

Creating users on OKTA

About this task

Use this procedure to add a user who requires SSO capabilities on OKTA.

Procedure

1. Log in to the OKTA administration portal as an administrator.
2. Navigate to **Directory > People**.
3. Click **Add Person**.
4. In **First Name**, type the first name of the user.
5. In **Last Name**, type the last name of the user.
6. In **Username**, type a unique identifier for the user.

You can use the user email address as a username.

7. In **Primary email**, type the same value as in **Username**.
8. In **Group**, select either the user group or the administrator group that you created.

The SSO capabilities are available to members of both groups. Select the administrator group if you want to provide the user with the administrator rights.

9. Click **Save**.

Adding users to groups

About this task

Each user who requires SSO capabilities must belong to a group that is assigned to the OKTA SAML application.

Before you begin

- Create a user group as described in [Configuring user and administrator groups](#) on page 80.
- Assign the group to the SAML application as described in [Assigning a group to an OKTA SAML application](#) on page 82.

Procedure

1. Log in to the OKTA administration portal as the administrator.
2. Navigate to **Directory > Groups**.
3. Select the either the user group or the administrator group that you created and then click **Manage People**.
Select the administrator group if you want to provide the user with the administrator rights.
4. Select users that you want to add to the group.
5. Click **Add All**.
6. Click **Save**.

Assigning a group to an OKTA SAML application

About this task

You must assign a group to the OKTA SAML v2.0 application that contains users requiring SSO capabilities.

Procedure

1. Log in to the OKTA administration portal as the administrator.
2. Navigate to **Application**.
3. Select your SAML application.
4. Go to **Assignments** tab.
5. Click **Assign** and then click **Assign to Groups**.
OKTA displays the list of available groups.
6. Click **Assign** for the group you want to assign to the application.
7. Click **Done**.

Configuring attribute mapping on OKTA

About this task

To authenticate a user, OKTA sends an authentication response to Keycloak containing various user attributes, such as the first name, last name, phone number, or email address. Keycloak then maps this user information to the attributes of the access token that is generated and sent back to clients. Use this procedure to specify Keycloak attribute names on OKTA.

Procedure

1. Log in to the OKTA administration portal as an administrator.
2. Navigate to **Directory > Profile Editor**.
3. Click **Profile** for your SAML v2.0 application.
4. On the Attributes page, click **Add Attribute** and add three new attributes with the following parameters:

Display Name	Variable Name	Data Type	Attribute Type
email	email	string	Custom
firstName	firstName	string	Custom
lastName	lastName	string	Custom

For other settings, leave default values.

The following image displays the configured email attribute:

Add Attribute

* Local app attributes are only stored on Okta and not created in aads. Use local attributes if you plan to add the attribute to aads or only want to store the mapped value in Okta.

Data type: string

Display name: email

Variable name: email

Description:

Enum: ☐ Define enumerated list of values

Attribute Length: Between

min:

and

max:

Attribute required: ☐ Yes

Scope: ☐ User personal

Buttons: Cancel, Save, Save and Add Another

5. Click **Save**.

6. On the **Attributes** page, click **Mappings**.
7. Navigate to the **<Your application name> to OKTA User** tab and then configure mapping as follows:

Table 1:

<Your Application Name> User Profile	OKTA User Profile
appuser.firstName	firstName
appuser.lastName	lastName
appuser.email	email

The following image displays the configured attributes:

8. Navigate to the **OKTA User to <your application name>** tab and then configure mapping as follows:

Table 2:

OKTA User Profile	<Your application name> User Profile
user.email	email
user.firstName	firstName
user.lastName	lastName

The following image displays the configured attributes:

9. Save mappings.
10. Navigate to **Application**.
11. Select your SAML application.
12. On the General tab, in the SAML Settings area, click **Edit**.
13. On the General Settings page, click **Next**.
14. On the Configure SAML page, select **Show Advanced Settings**.
15. In the Attribute Statements area, add attribute statements as follows:

Name	Name format	Value
email	Unspecified	user.email
firstName	Unspecified	user.firstName
lastName	Unspecified	user.lastName

The following image displays the configured attributes:

16. In the Group Attribute Statements area, add group attribute statements as follows:

Name	Name format	Filter	Value
Admin	Unspecified	Equals	The name of the administrator group configured on OKTA.

Name	Name format	Filter	Value
User	Unspecified	Equals	The name of the user group configured on OKTA.

The following image displays the configured attributes:

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter	Value
Admin	Unspecified	Equals	Admin
User	Unspecified	Equals	User

Add Another

17. Click **Next**.

18. Click **Save**.

Avaya Aura Device Services integration with Microsoft AD FS

Checklist for configuring AD FS integration using SAML v2.0

The following checklist lists the configuration tasks that you perform on the Keycloak and AD FS web administration portals to set up integration with Microsoft Active Directory Federation Services (AD FS) using SAML v2.0.

No.	Task	Notes	✓
1	Ensure that you gather all required information for configuring the integration.	See Prerequisites for SSO configuration on page 52.	
2	Enable and configure SSO functionality on AD FS.	See the Microsoft documentation for AD FS installation and configuration.	
3	Obtain the AD FS configuration file.	See the prerequisites in Configuring an AD FS SAML v2.0 identity provider on Keycloak on page 88.	
4	Configure Keycloak settings using the Avaya Aura® Device Services configuration utility.	See Configuring Keycloak settings on page 124.	

No.	Task	Notes	✓
5	Configure the AD FS identity provider on Keycloak.	See Configuring an AD FS SAML v2.0 identity provider on Keycloak on page 88.	
6	Configure Keycloak as a relying party trust on AD FS.	See Configuring Keycloak as a relying party trust on page 88.	
7	Configure attribute mapping between the AD FS SAML v2.0 identity provider and Keycloak.	See Modifying the attribute mapping between the third-party identity provider and Keycloak on page 133. For information about mappers that you must configure on Keycloak, see Attribute mapping parameters for ADFS SAML v2.0 identity provider on page 138.	
8	Configure the claim issuance policy on AD FS.	See Configuring the claim issuance policy on page 89.	
9	Obtain the client secret.	See Obtaining the client secret on page 126. The client secret is required to enable communication between Avaya Aura® Device Services and Keycloak.	
10	Create a client mapping.	See Creating client mapping on page 126. If you need to regenerate the client secret, see Regenerating the Keycloak client secret on page 129.	
11	Configure the LDAP UID mapping.	See Configuring the LDAP UID mapping on page 144.	
12	Select the identity provider to use for authorization.	See Selecting the default identity provider on page 132. Do not perform this task if you want to allow the simultaneous use of multiple identity providers to your enterprise users.	
13	Test the integration with AD FS.	See Testing the integration with the identity provider from the web administration portal on page 147.	
14	Configure expiry time for access and refresh tokens.	See Configuring access and refresh token expiry times on page 149.	

Configuring an AD FS SAML v2.0 identity provider on Keycloak

About this task

To use the Microsoft AD FS SSO capabilities and authenticate users, you must configure a SAML v2.0 identity provider on Keycloak.

Before you begin

- Configure an AD FS SAML application.
- Obtain a configuration metadata file in XML format from AD FS using the following URL: `https://<ADFS IP or FQDN>/FederationMetadata/2007-06/FederationMetadata.xml`.

Procedure

1. Log in to the Keycloak web administration interface.
2. Navigate to **Solution Realm > Identity Providers**.
3. Click **Add provider** and then select **SAML v2.0**.
4. In **Alias**, type the name that you used when configuring an SAML application on the AD FS management console.

For example, `adfsSAML`.

5. Navigate to the Import External IDP Config section.
6. Click **Select file**, navigate to the AD FS configuration metadata XML file that is stored on your computer, and then click **Import**.

Keycloak imports the configuration data and populates the **Single Sign-On Service URL** field.

7. From **NameID Policy Format**, select **Email**.
8. Click **Save**.

Configuring Keycloak as a relying party trust

About this task

Use this procedure to add Keycloak to AD FS as a relying party trust. This is required to allow Keycloak to redirect clients to AD FS for authentication.

Before you begin

Download the descriptor metadata file in XML format from Keycloak using the following URL: `https://<AADS FQDN or IP>/auth/realms/SolutionRealm/broker/<SAML IDP name>/endpoint/descriptor`.

Procedure

1. Log in to the AD FS Manager as an administrator.
2. Navigate to **Relying Party Trust**.

3. On the right side of the screen, select **Add Relying Party Trust**.
AD FS Manager displays the Add Relying Party Trust wizard.
4. On the Welcome page of the wizard, select **Claim aware** and then click **Start**.
5. On the Select Data Source page, select **Import data about the relying party from a file**.
6. Click **Browse** and then select the descriptor metadata file in XML format that you downloaded from Keycloak.
7. Click **Next**.
8. On the Specify Display Name page, in **Display Name**, type a name of your choice for the relying party.
9. On the Choose Access Control Policy page, select **Permit everyone** and then click **Next**.
10. Click **Next** again and then click **Finish**.

Configuring the claim issuance policy

About this task

AD FS issues tokens that contain set of claims. You must configure the claim issuance policy so that AD FS passes correct claims to Keycloak and receives correct claims from Keycloak.

Procedure

1. Log in to the AD FS Manager as an administrator.
2. Navigate to **Relying Party Trust**.
3. Right click on the relying party that you created for Keycloak and then select **Edit Claim Issuance Policy** from the menu.
4. Click **Add Rule** and add a new rule with the following parameters:
 - a. In **Rule template**, select **Send LDAP Attributes as Claim**.
 - b. In **Claim rule name**, type a name of your choice for the rule.
 - c. In **Attribute store**, select **Active Directory**.
 - d. Configure the mapping of LDAP attributes to outgoing claim types as in the following table:

LDAP Attribute	Outgoing Claim Type
Given-Name	Given Name
Surname	Surname
E-Mail-Addresses	E-Mail Address

5. Click **Add Rule** and add a new rule with the following parameters:
 - a. In **Rule template**, select **Transform an Incoming Claim**.
 - b. In **Claim rule name**, type `Name ID`.

- c. In **Incoming claim type**, select **E-Mail Address**.
 - d. In **Outgoing claim type**, select **Name ID**.
 - e. In **Outgoing name ID format**, select **Email**.
 - f. Select **Pass through all claim values**.
6. Click **Add Rule** and add a new rule with the following parameters:
- a. In **Rule template**, select **Send Group Membership as a Claim**.
 - b. In **Claim rule name**, type `Group: user`.
 - c. In **User's group**, select a group with users who must use SSO capabilities from your active directory.
 - d. In **Outgoing claim type**, select **Group**.
 - e. In **Outgoing claim value**, select **user**.
7. Click **Add Rule** and add a new rule with the following parameters:
- a. In **Rule template**, select **Send Group Membership as a Claim**.
 - b. In **Claim rule name**, type `Group: admin`.
 - c. In **User's group**, select a group with administrative users from your active directory.
 - d. In **Outgoing claim type**, select **Group**.
 - e. In **Outgoing claim value**, select **admin**.

Avaya Aura Device Services integration with One Login

Checklist for configuring OneLogin integration using SAML v2.0

The following checklist lists the configuration tasks that you perform to set up integration with OneLogin using SAML v2.0.

No.	Task	Notes	✓
1	Ensure that you gather all required information for configuring the integration.	See Prerequisites for SSO configuration on page 52.	
2	Enable and configure SSO functionality on OneLogin and obtain the configuration file.	See Creating a new SAML v2.0 application on OneLogin on page 92.	
3	Configure Keycloak settings using the Avaya Aura® Device Services configuration utility.	See Configuring Keycloak settings on page 124.	

No.	Task	Notes	✓
4	Configure the OneLogin identity provider on Keycloak.	See Configuring a OneLogin SAML v2.0 identity provider on Keycloak on page 93.	
5	Configure attribute mapping on OneLogin.	See Configuring attribute mapping on OneLogin on page 93.	
6	Configure attribute mapping between the OneLogin SAML v2.0 identity provider and Keycloak.	See Modifying the attribute mapping between the third-party identity provider and Keycloak on page 133. For information about mappers that you must configure on Keycloak, see Attribute mapping parameters for OneLogin SAML v2.0 identity provider on page 139.	
7	Create users on OneLogin.	See Creating users on OneLogin on page 94.	
8	Obtain the client secret.	See Obtaining the client secret on page 126. The client secret is required to enable communication between Avaya Aura® Device Services and Keycloak.	
9	Create a client mapping.	See Creating client mapping on page 126. If you need to regenerate the client secret, see Regenerating the Keycloak client secret on page 129.	
10	Configure the LDAP UID mapping.	See Configuring the LDAP UID mapping on page 144.	
11	Select the identity provider to use for authorization.	See Selecting the default identity provider on page 132. Do not perform this task if you want to allow the simultaneous use of multiple identity providers to your enterprise users.	
12	Test the integration with OneLogin.	See Testing the integration with the identity provider from the web administration portal on page 147.	
13	Configure expiry time for access and refresh tokens.	See Configuring access and refresh token expiry times on page 149.	

Creating a new SAML v2.0 application on OneLogin

About this task

Use this procedure to configure a new application for SSO on OneLogin using the OneLogin administration console.

When configuring the application, you obtain an identity provider alias and configuration file. You will need this data later when configuring a OneLogin SAML v2.0 identity provider on Keycloak.

Before you begin

Register an account on OneLogin.

Procedure

1. Log in to the OneLogin administration console as an administrator.
2. Navigate to **Applications > Applications**.
3. On the Applications page, click **Add app**.
4. From the application list, select **SAML Test Connector (Advanced)** with the **SAML 2.0** application type.
5. In **Display Name**, type a name for your SAML 2.0 application.
6. Click **Save**.
7. Navigate to **Applications > Applications** and then select the application that you created.
8. On the application page, navigate to the **Configuration** tab and then configure the settings as follows:
 - a. In **RelayState**, type `https://<AADS_FQDN>/auth/realms/SolutionRealm`.
In this string, <AADS_FQDN> is the Avaya Aura® Device Services front-end FQDN.
 - b. In **Audience (EntityID)**, type `https://<AADS_FQDN>/auth/realms/SolutionRealm`.
 - c. In **ACS (Consumer) URL Validator**, type `https://<AADS_FQDN>/auth/realms/SolutionRealm/broker/<IDP_ALIAS>/endpoint`.
In this string, <IDP_ALIAS> is an identity provider alias of your choice. For example, OneLoginSAML.
 - d. In **ACS (Consumer) URL**, type `https://<AADS_FQDN>/auth/realms/SolutionRealm/broker/<IDP_ALIAS>/endpoint`.
 - e. In **Login URL**, type `https://<AADS_FQDN>/auth/realms/SolutionRealm/broker/<IDP_ALIAS>/endpoint`.
 - f. In **SAML nameID format**, select **Email**.
 - g. Leave default values for all other fields.
9. Remember the identity provider alias that you used in the previous step.

You will use this alias later when creating a Ping Identity SAML v2.0 provider on Keycloak.

10. Click **Save**.
11. On the application page, from **More Actions**, select **SAML Metadata** and save the `onelogin_metadata_#####.xml` configuration file on your computer.

Configuring a OneLogin SAML v2.0 identity provider on Keycloak

About this task

To use OneLogin SSO capabilities and authenticate users, you must configure a SAML v2.0 identity provider on Keycloak.

Before you begin

- Configure a SAML application on OneLogin.
- Obtain a configuration file in XML format.

Procedure

1. Log in to the Keycloak web administration interface.
2. Navigate to **Solution Realm > Identity Providers**.
3. Click **Add provider** and then select **SAML v2.0**.
4. In **Alias**, type the name that you used when configuring a SAML application on OneLogin.
For example, `OneLoginSAML`. For more information, see step 8 on page 92.
5. In **Display name**, type a name of your choice.
6. Navigate to the Import External IDP Config section.
7. Click **Select file**, navigate to the OneLogin configuration metadata XML file that is stored on your computer, and then click **Import**.

Keycloak imports the configuration data and populates the **Single Sign-On Service URL** field.
8. From **NameID Policy Format**, select **Email**.
9. Click **Save**.

Configuring attribute mapping on OneLogin

About this task

To authenticate a user, OneLogin sends an authentication response to Keycloak containing various user attributes, such as the first name, last name, phone number, or email address. Keycloak then maps this user information to the attributes of the access token that is generated and sent back to clients.

You must configure the following attributes on OneLogin:

OneLogin attribute name	Attribute value
email	Email

OneLogin attribute name	Attribute value
firstName	First Name
lastName	Last Name
Group	No default

Procedure

1. Log in to the OneLogin administration console as an administrator.
2. Navigate to **Application** and then select your SAML 2.0 application.
3. Navigate to the **Parameters** tab.
4. Configure new attributes as follows:
 - a. Click the **Plus** icon to create a new attribute.
 - b. In **Field Name**, type the name from the “OneLogin attribute name” column of the table.
 - c. Select the **Include in SAML assertion** check box.
 - d. Click **Save**.
 - e. In **Edit Field**, select the value specified for the parameter in the “Attribute value” column.
 - f. Click **Save**.
 - g. Repeat substeps a to f to add other attributes.
5. Click **Save**.

Creating users on OneLogin

About this task

Use this procedure to add a user who requires SSO capabilities on OneLogin.

You can review the created users by navigating to **Applications > <Your application name> > User**.

Procedure

1. Log in to the OneLogin administration console as an administrator.
2. Navigate to **Users > Users**.
3. Click **New User**.
4. In **First Name**, type the first name of the user.
5. In **Last Name**, type the last name of the user.
6. In **Email**, type the email address of the user.
7. Select the **Active** check box.
8. Click **Save**.

9. On the user's page, navigate to the **Applications** tab.
10. In the Applications area, click the **Plus** icon.
11. From the list of applications, select your SAML 2.0 application, and then click **Continue**.
12. In **Group**, enter one of the following group names:
 - **admin**: Type this value if you want to provide the administrator rights to the user.
 - **user**: Type this value if you do not want to provide administrator rights to the user.

The SSO capabilities are available to members of both these groups.

13. Click **Save**.
14. Click **Save User**.

Avaya Aura Device Services integration with IBM SVA

Checklist for configuring IBM SVA integration using SAML v2.0

The following checklist lists the configuration tasks that you perform on the IBM Security Verify Access (SVA) and Keycloak web administration portals to set up integration with IBM SVA using SAML v2.0.

No.	Task	Notes	✓
1	Ensure that you gather all required information for configuring the integration.	See Prerequisites for SSO configuration on page 52.	
2	Create and configure an application for SSO using the IBM SVA administration dashboard and obtain the configuration metadata file.	See Creating a new SAML v2.0 application on IBM SVA on page 96.	
3	Configure Keycloak settings using the Avaya Aura® Device Services configuration utility.	See Configuring Keycloak settings on page 124.	
4	Configure an IBM SVA identity provider on Keycloak.	See Configuring an IBM SVA SAML v2.0 identity provider on Keycloak on page 98.	
5	Configure user and administrator groups on IBM SVA.	See Configuring user and administrator groups on page 98.	
6	Assign the groups to the SAML application on IBM SVA.	See Assigning groups to your IBM SVA SAML application on page 99.	
7	Configure attribute mapping on IBM SVA.	See Configuring attribute mapping on IBM SVA on page 100.	

No.	Task	Notes	✓
8	Configure attribute mapping between the IBM SVA SAML v2.0 identity provider and Keycloak.	See Modifying the attribute mapping between the third-party identity provider and Keycloak on page 133. For information about mappers that you must configure on Keycloak, see Attribute mapping parameters for the IBM SVA SAML v2.0 identity provider on page 139.	
9	Obtain the client secret.	See Obtaining the client secret on page 126. The client secret is required to enable communication between Avaya Aura® Device Services and Keycloak.	
10	Create a client mapping.	See Creating client mapping on page 126. If you need to regenerate the client secret, see Regenerating the Keycloak client secret on page 129.	
11	Configure the LDAP UID mapping.	See Configuring the LDAP UID mapping on page 144.	
12	Select the identity provider to use for authorization.	See Selecting the default identity provider on page 132. Do not perform this task if you want to allow the simultaneous use of multiple identity providers to your enterprise users.	
13	Create users on IBM SVA.	See Creating users on IBM SVA on page 101.	
14	Add users to the groups on IBM SVA.	See Adding users to groups on page 101.	
15	Test the integration with IBM SVA.	See Testing the integration with the identity provider from the web administration portal on page 147.	
16	Configure expiry time for access and refresh tokens.	See Configuring access and refresh token expiry times on page 149.	

Creating a new SAML v2.0 application on IBM SVA

About this task

Use this procedure to configure a new application for SSO on IBM Security Verify Access (SVA) using the IBM SVA Administration dashboard.

When configuring the application, you obtain an identity provider alias and configuration file. You need this data later when configuring an IBM SVA SAML v2.0 identity provider on Keycloak.

Before you begin

Register an account on IBM SVA.

Procedure

1. Log in to the IBM SVA Administration dashboard as the administrator.
2. In the left navigation pane, navigate to **Applications**.
3. On the Applications page, click **Add Application**.
4. In the Select Application Type window, select **Custom Application** and then click **Add application**.

The IBM SVA Administration dashboard displays the Add Application page.

5. On the General tab, type a name of your choice for your SAML 2.0 application.
6. In **Company name**, type the name of your company.
7. Click **Add owner**.
8. In the **Select user** window, select a user that you want to make an owner of the application, and then click **OK**.
9. On the Add Application page, go to the **Sign-on** tab and complete the following fields:
 - a. In **Sign-on method**, select **SAML2.0**.
 - b. In **Assertion consumer service URL (HTTP-POST)**, type `https://<AADS_FQDN>/auth/realms/SolutionRealm/broker/<IDP_ALIAS>/endpoint`.

 <AADS_FQDN> is the Avaya Aura® Device Services front-end FQDN. <IDP_ALIAS> is an identity provider alias of your choice. For example, SVAsaml.
 - c. In **Provider ID**, type `https://<AADS_FQDN>/auth/realms/SolutionRealm`.
 - d. Select the **Use identity provider initiated single sign-on** check box.
 - e. In **Target URL**, type `https://<AADS_FQDN>/auth/realms/SolutionRealm/broker/<IDP_ALIAS>/endpoint`.
 - f. In **Service provider SSO URL**, type `https://<AADS_FQDN>/auth/realms/SolutionRealm/broker/<IDP_ALIAS>/endpoint`.
 - g. Select the **Sign authentication response** check box.
 - h. In **Signature algorithm**, select **RSA-SHA256**.
 - i. In **Name identifier**, select **preferred_username**.
 - j. In **NameID format**, select **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.
 - k. Leave default values for all other fields.

10. Remember the identity provider alias that you used in the previous step.

You use this alias later when creating a Ping Identity SAML v2.0 provider on Keycloak.

11. Click **Save**.

12. In the right navigation pane, navigate to the Upload the identity provider federation metadata, which you can download from the following URL step and then click the link to download the configuration file in XML format.

Configuring an IBM SVA SAML v2.0 identity provider on Keycloak

About this task

To use IBM SVA SSO capabilities and authenticate users, you must configure a SAML v2.0 identity provider on Keycloak.

Before you begin

- Configure an SAML application on IBM SVA Administration dashboard.
- Obtain a configuration metadata file in XML format.

Procedure

1. Log in to the Keycloak web administration interface.
2. Navigate to **Solution Realm > Identity Providers**.
3. Click **Add provider** and then select **SAML v2.0**.
4. In **Alias**, type the name that you used when configuring a SAML application on IBM SVA.
For example, `SVAsaml`. For more information, see step [9.b](#) on page 97.
5. Navigate to the Import External IDP Config section.
6. Click **Select file**, navigate to the IBM SVA configuration XML file that is stored on your computer, and then click **Import**.
Keycloak imports the configuration data and populates the **Single Sign-On Service URL** field.
7. From **NameID Policy Format**, select **Email**.
8. Click **Save**.

Configuring user and administrator groups

About this task

A group defines a set of users on IBM SVA. You must create the following groups on IBM SVA:

- User group.
- Administrator group, which is used for administration purposes.

You also use these group settings to configure attribute mapping between IBM SVA and Keycloak.

 Note:

The SSO capabilities are available to members of both these groups.

Procedure

1. Log in to the IBM SVA Administration dashboard as the administrator.
2. In the left navigation pane, navigate to **User&group**.
3. Click the **Groups** tab.
4. Create an administrator group as follows:
 - a. Click **Add group**.
 - b. In **Name**, type a name of your choice for the group.
For example, `Admin`.
 - c. **(Optional)** In **Description**, provide a description for the group.
 - d. Click **Save**.
IBM SVA displays information about the created group.
 - e. Remember the name of the group.
You use this value later when configuring attribute mapping on Keycloak.
5. Create a user group as follows:
 - a. Click **Add group**.
 - b. In **Name**, type a name of your choice for the group.
For example, `User`.
 - c. **(Optional)** In **Description**, provide a description for the group.
 - d. Click **Save**.
IBM SVA displays information about the created group.
 - e. Remember the name of the group.
You use this value later when configuring attribute mapping on Keycloak.

Assigning groups to your IBM SVA SAML application

About this task

You must assign a group to the IBM SVA SAML v2.0 application that contains users requiring SSO capabilities.

Before you begin

- Create a SAML application on IBM SVA as described in [Creating a new SAML v2.0 application on IBM SVA](#) on page 96.
- Create the required user groups as described in [Configuring user and administrator groups](#) on page 98.

Procedure

1. Log in to the IBM SVA Administration dashboard as the administrator.
2. In the left navigation pane, navigate to **App role management**.
3. On the App role management page, click the **Permissions** tab.
4. Select your SAML application and then click **Manage membership**.
5. On the Basic access page, click the **Groups** tab.
6. Click **Assign new groups**.
7. Select the user group and the administration group that you created and then click **Add group**.

Configuring attribute mapping on IBM SVA

About this task

To authenticate a user, IBM SVA sends an authentication response to Keycloak containing various user attributes, such as the first name, last name, phone number, or email address. Keycloak then maps this user information to the attributes of the access token that is generated and sent back to clients.

Procedure

1. Log in to the IBM SVA Administration dashboard as an administrator.
2. Navigate to **Application** and then select your SAML 2.0 application.
3. Click the **Settings** icon to the right of your application name.
4. Select the **Sign-on** tab.
5. In the Attribute mappings area, select the **Send all known user attributes in the SAML assertion** check box.
6. Configure new attributes as described in the following table:

Attribute name	Attribute name file format	Attribute source
firstName	urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified	family_name
lastName	urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified	given_name
email	urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified	email
group	urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified	groupIds

7. Click **Save**.

Creating users on IBM SVA

About this task

Use this procedure to add a user who requires SSO capabilities on IBM SVA.

Procedure

1. Log in to the IBM SVA Administration dashboard as the administrator.
2. In the left navigation pane, navigate to **User&group**.
3. Click the **Users** tab.
4. Click **Add user**.

The IBM SVA Administration dashboard displays the Add user window.

5. In **Identity source**, select **Cloud Directory**.
6. In **Status**, select **On**.
7. In **Given Name**, type the first name of the user.
8. In **Surname**, type the last name of the user.
9. In **User name**, type a unique identifier for the user.
10. In **Work e-mail**, type the email address of the user.

IBM SVA sends the user password to this email address. The user can change the password on the first login.

11. **(Optional)** Complete other fields on the Add user as appropriate.
12. Click **Save**.

Adding users to groups

About this task

Each user who requires SSO capabilities must belong to a group that is assigned to the IBM SVA SAML application.

Before you begin

Create groups as described in [Configuring user and administrator groups](#) on page 98.

Procedure

1. Log in to the IBM SVA Administration dashboard as the administrator.
2. In the left navigation pane, go to **User&group**.
3. Click the **Groups** tab.
4. Select an appropriate group and then click **Edit**.

The IBM SVA Administration dashboard displays the Edit group page.

5. In the Group members area, click **Add**.

6. Select users that you want to add to the group.
7. Click **Select**.
8. After adding all required users to the group, click **Done**.

Avaya Aura Device Services integration with Duo

Checklist for configuring Duo integration using SAML v2.0

The following checklist lists the configuration tasks that you perform on the Duo Access Gateway (DAG), Duo Admin Panel, and Keycloak web administration portals to set up integration with Duo using SAML v2.0.

No.	Task	Notes	✓
1	Ensure that you gather all required information for configuring the integration.	See Prerequisites for SSO configuration on page 52.	
2	Deploy DAG in your environment and ensure that you can access the Duo Security Service domain duosecurity.com from DAG.	See the documentation for DAG at https://duo.com/docs/dag .	
3	Create and configure an SAML application for SSO using the Duo Admin Panel.	See Creating a new SAML v2.0 application on Duo on page 103.	
4	Add the SAML application to DAG and obtain the configuration metadata file.	See Adding your SAML application to the Duo Access Gateway on page 104.	
5	Configure Keycloak settings using the Avaya Aura® Device Services configuration utility.	See Configuring Keycloak settings on page 124.	
6	Configure a Duo identity provider on Keycloak.	See Configuring a Duo SAML v2.0 identity provider on Keycloak on page 105.	
7	Configure attribute mapping between the Duo SAML v2.0 identity provider and Keycloak.	See Modifying the attribute mapping between the third-party identity provider and Keycloak on page 133. For information about mappers that you must configure on Keycloak, see Attribute mapping parameters for the Duo SAML v2.0 identity provider on page 140.	

No.	Task	Notes	✓
8	Obtain the client secret.	See Obtaining the client secret on page 126. The client secret is required to enable communication between Avaya Aura® Device Services and Keycloak.	
9	Create a client mapping.	See Creating client mapping on page 126. If you need to regenerate the client secret, see Regenerating the Keycloak client secret on page 129.	
10	Configure the LDAP UID mapping.	See Configuring the LDAP UID mapping on page 144.	
11	Select the identity provider to use for authorization.	See Selecting the default identity provider on page 132. Do not perform this task if you want to allow the simultaneous use of multiple identity providers to your enterprise users.	
12	Test the integration with Duo.	See Testing the integration with the identity provider from the web administration portal on page 147.	
13	Configure expiry time for access and refresh tokens.	See Configuring access and refresh token expiry times on page 149.	

Creating a new SAML v2.0 application on Duo

About this task

Use this procedure to configure a new application for SSO on Duo using the Duo administration portal.

When configuring the application, you obtain an identity provider alias and configuration file. You need this data later when configuring an Duo SAML v2.0 identity provider on Keycloak.

Before you begin

- Deploy the Duo Access Gateway (DAG).
- Configure the authentication source on DAG.

For information, see the Duo documentation.

Procedure

1. Log in to the Duo Admin Panel as an administrator.
2. In the left navigation pane, click **Applications** and then click **Protect an Application**.
3. Click **Protect an Application** again.

4. In the application list, navigate to the **Generic Service Provider** entry that has the “2FA with SSO self-hosted (Duo Access Gateway)” protection type.
5. On the right side of the entry, click **Protect**.
6. In the Service Provider section, complete the following fields:
 - a. In **Service Provider Name**, type a name of your choice for your SAML 2.0 application.
 - b. In **Assertion Consumer Service**, type `https://<AADS_FQDN>/auth/realms/SolutionRealm/broker/<IDP_ALIAS>/endpoint`.

 <AADS_FQDN> is the Avaya Aura® Device Services front-end FQDN. <IDP_ALIAS> is an identity provider alias of your choice. For example, `samlDuo`.
 - c. In **Entity ID**, type `https://<AADS_FQDN>/auth/realms/SolutionRealm`.
 - d. Leave default values for all other fields.
7. Remember the identity provider alias that you used in the previous step.
 You use this alias later when creating a Ping Identity SAML v2.0 provider on Keycloak.
8. In the SAML Response section, complete the following fields:
 - a. In **NameID format**, select **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.
 - b. In **NameID attribute**, select **mail**.
 - c. In **Send attributes**, select **NameID**.
 - d. In **Signature algorithm**, select **SHA-256**.
 - e. Leave default values for all other fields.
9. Click **Save Configuration**.
10. In the Configure SAML Service Provider area, click **Download your configuration file** to download the configuration file in JSON format and save the file on your computer.

Adding your SAML application to the Duo Access Gateway

About this task

Duo Access Gateway (DAG) acts as an identity provider, authenticating users using their authentication resource credentials. DAG uses the SAML 2.0 authentication standard to authenticate users. To use DAG authentication capabilities, you must register your SAML 2.0 application on DAG.

Before you begin

- Create an SAML 2.0 application on Duo Admin Panel.
- Ensure that you have the configuration file in JSON format for your SAML 2.0 application.

Procedure

1. Log in to the DAG administration portal as the administrator.
2. In the left navigation pane, click **Applications**.
3. In the Add Application section, click **Choose File** and then select the configuration file in JSON format for your SAML 2.0 application.
4. Click **Upload**.

DAG displays your SAML 2.0 application in the Applications area.

5. Navigate to the **Metadata** area, click **Download XML metadata**, and save the configuration metadata file in XML format on your computer.

Configuring a Duo SAML v2.0 identity provider on Keycloak

About this task

To use Duo SSO capabilities and authenticate users, you must configure a SAML v2.0 identity provider on Keycloak.

Before you begin

- Add your SAML application to DAG.
- Obtain a configuration metadata file in XML format.

Procedure

1. Log in to the Keycloak web administration interface.
2. Navigate to **Solution Realm > Identity Providers**.
3. Click **Add provider** and then select **SAML v2.0**.
4. In **Alias**, type the name that you used when configuring a SAML application on Duo Admin Panel.

For example, `samlDuo`. For more information, see step [6.b](#) on page 104.

5. Navigate to the Import External IDP Config section.
6. Click **Select file**, navigate to the Duo configuration XML file that is stored on your computer, and then click **Import**.

Keycloak imports the configuration data and populates the **Single Sign-On Service URL** field.

7. From **NameID Policy Format**, select **Email**.
8. Click **Save**.

Avaya Aura Device Services integration with Imprivata

Checklist for configuring Imprivata integration using SAML v2.0

The following checklist lists the configuration tasks that you must perform to set up the integration with the Imprivata identity provider.

No.	Task	Notes	✓
1	Ensure that you gather all required information for configuring the integration.	See Prerequisites for SSO configuration on page 52.	
2	Contact Imprivata support to configure SSO functionality for your company on Imprivata.	Provide the name of the domain that you are planning to use for authorization to Imprivata. Users that belong to this domain can use Imprivata SSO functionality.	
3	Obtain the metadata file in XML format from Imprivata.		
4	Configure LDAP settings.	See Configuring LDAP settings on page 107.	
5	Enable role fetching from LDAP.	See Enabling role fetching from LDAP on page 107.	
6	Configure Keycloak settings using the Avaya Aura® Device Services configuration utility.	See Configuring Keycloak settings on page 124.	
7	Configure an Imprivata identity provider on Keycloak.	See Configuring an Imprivata SAML v2.0 identity provider on Keycloak on page 108.	
8	Configure attribute mapping between the Imprivata SAML v2.0 identity provider and Keycloak.	See Modifying the attribute mapping between the third-party identity provider and Keycloak on page 133. For information about mappers that you must configure on Keycloak, see Attribute mapping parameters for Imprivata SAML v2.0 identity provider on page 141.	
9	Download the SPSSODescriptor metadata file from Keycloak and provide it to Imprivata.	See Downloading the SPSSODescriptor file from Keycloak on page 108.	

No.	Task	Notes	✓
10	Select the identity provider to use for authorization.	See Selecting the default identity provider on page 132. Do not perform this task if you want to allow the simultaneous use of multiple identity providers to your enterprise users.	
11	Test the integration with Imprivata.	See Testing the integration with the identity provider from the web administration portal on page 147.	
12	Configure expiry time for access and refresh tokens.	See Configuring access and refresh token expiry times on page 149.	

Configuring LDAP settings

About this task

You must enable the authentication functionality for the LDAP server that contains the domain that you plan to use for integration with Imprivata. You must also set this domain as the authentication domain of the LDAP server.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
2. Select the LDAP server that contains the domain that you plan to use for integration with Imprivata authentication.
3. Select the **Use for authentication** check box.
4. Ensure that **Authentication Domain** contains the name of the domain that you plan to use for integration with Imprivata.
5. If **Authentication Domain** contains another domain name, do the following:
 - a. Select the **Edit Domain** check box.
 - b. In **Authentication Domain** type the name of the domain that you use for integration with Imprivata.
6. Click **Save**.

Enabling role fetching from LDAP

About this task

The Imprivata identity provider does not provide the required user roles for user role mapping. You must configure Avaya Aura® Device Services to fetch the roles directly from LDAP.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **System Parameters > Parameter Configuration**.
2. In **FETCH_ROLE_FROM_LDAP**, select **True**.
3. Click **Save**.

Configuring an Imprivata SAML v2.0 identity provider on Keycloak

About this task

To use Imprivata SSO capabilities and authenticate users, you must configure a SAML v2.0 identity provider on Keycloak.

Before you begin

- Contact Imprivata to configure SSO functionality for your enterprise on the Imprivata side.
- Obtain a configuration metadata file in XML format from Imprivata.

Procedure

1. Log in to the Keycloak web administration interface.
2. Navigate to **Solution Realm > Identity Providers**.
3. Click **Add provider** and then select **SAML v2.0**.
4. In **Alias**, type a name of your choice.
For example, `ImprivataSAML`.
5. Navigate to the Import External IDP Config section.
6. Click **Select file**, navigate to the Imprivata configuration XML file that is stored on your computer, and then click **Import**.

Keycloak imports the configuration data and populates the **Single Sign-On Service URL** field.

7. From **NameID Policy Format**, select **Email**.
8. Click **Save**.

Downloading the SPSSODescriptor file from Keycloak

About this task

After you configure identity provider settings on Keycloak, it generates an SPSSODescriptor metadata file for this provider. Provide this file to the identity provider to complete the configuration process.

Before you begin

Configure the identity provider on Keycloak.

Procedure

1. In a web browser, navigate to the following URL:

`https://<AADS_FQDN>:<AADS_PORT>/auth/realms/SolutionRealm/broker/<ALIAS>/endpoint/descriptor`

In this URL:

- <AADS_FQDN> is the Avaya Aura® Device Services front-end FQDN.
 - <AADS_PORT> is the Avaya Aura® Device Services front-end port.
 - <SAML_ALIAS> is the alias of the identity provider. You set up this name when configuring the identity provider settings on Keycloak.
2. Save the SPSSODescriptor file on your computer.

Avaya Aura Device Services integration with Auth0

Checklist for configuring Auth0 integration using SAML v2.0

The following checklist lists the configuration tasks that you perform on Auth0 and the Keycloak web administration portal to set up integration with Auth0 using SAML v2.0.

No.	Task	Notes	✓
1	Ensure that you gathered all required information for configuring integration.	See Prerequisites for SSO configuration on page 52.	
2	Create and configure an application for SSO on Auth0 Dashboard and obtain the configuration metadata file.	See Creating a new application on page 110.	
3	Configure Keycloak settings using the Avaya Aura® Device Services configuration utility.	See Configuring Keycloak settings on page 124.	
4	Create a rule to set up first name and last name attributes in the user's profile on Auth0.	See Setting up last name and first name attributes in the user's profile on page 114.	
5	Configure users on Auth0.	See Creating users on Auth0 on page 113.	
6	Configure an Auth0 SAML v2.0 identity provider on Keycloak.	See Configuring an Auth0 SAML v2.0 identity provider on Keycloak on page 112.	

No.	Task	Notes	✓
7	Configure attribute mapping between Auth0 and Keycloak.	See Modifying the attribute mapping between the third-party identity provider and Keycloak on page 133. For information about mappers that you must configure on Keycloak, see Attribute mapping parameters for Auth0 SAML v2.0 identity provider on page 141.	
8	Obtain the client secret.	See Obtaining the client secret on page 126. The client secret is required to enable communication between Avaya Aura® Device Services and Keycloak.	
9	Create a client mapping.	See Creating client mapping on page 126. If you need to regenerate the client secret, see Regenerating the Keycloak client secret on page 129.	
10	Configure the LDAP UID mapping.	See Configuring the LDAP UID mapping on page 144.	
11	Select the identity provider to use for authorization.	See Selecting the default identity provider on page 132. Do not perform this task if you want to allow the simultaneous use of multiple identity providers to your enterprise users.	
12	Test the integration with Auth0.	See Testing the integration with the identity provider from the web administration portal on page 147.	
13	Configure expiry time for access and refresh tokens.	See Configuring access and refresh token expiry times on page 149.	

Creating a new application

About this task

Use this procedure to configure a new application for SSO on Auth0.

When configuring the application, you obtain an identity provider alias and configuration file. You will need this data later when configuring an Auth0 identity provider on Keycloak.

For more information about creating applications on the Auth0 Dashboard, see [Create applications](#).

Before you begin

Ensure that you have an administrative account and a tenant on Auth0. For information about creating tenants, see [Create tenants](#). For information about the pricing plans, see <https://auth0.com/pricing>.

Procedure

1. Log in to the Auth0 Dashboard at <https://manage.auth0.com/> as an administrator.
2. Navigate to **Applications > Applications**.
3. On the Applications page, click **Create application**.
4. In **Name**, type a name of your choice for the application.
5. In **Choose an application type**, select **Native**.
6. Click **Create**.
7. Navigate to the **Applications** page again and click the application that you have just created.
8. On the Application properties page, click the **Settings** tab.
9. In the Application URIs section, configure the following settings:
 - a. In **Application Login URI** and **Allowed Callback URLs**, type `https://<AADS_FQDN>/auth/realms/SolutionRealm/broker/<IDP_ALIAS>/endpoint`.

In these strings, <AADS_FQDN> is the Avaya Aura® Device Services front-end FQDN. <IDP_ALIAS> is an identity provider alias of your choice. For example, Auth0SAML.
 - b. Leave default values for other fields.
10. Click **Save changes**.
11. Click the **Connections** tab.
12. In the Social section, disable the **google-oauth2** option.
13. Click the **Addons** tab.
14. Click the **SAML2 WEB APP** slider to enable the SAML2 Web App add-on.
15. On the Addon: SAML2 Web App page, click the **Settings** tab.
16. In **Application Callback URL**, type `https://<AADS_FQDN>/auth/realms/SolutionRealm/broker/<IDP_ALIAS>/endpoint`.

In this string, <AADS_FQDN> is the Avaya Aura® Device Services front-end FQDN. <IDP_ALIAS> is the identity provider alias that you used in step 9 on page 111.
17. In **Settings**, type the following to configure attribute mapping:

```
{
  "mappings": {
    "email": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress",
    "given_name": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname",
  }
}
```

```

    "family_name": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname",
    "roles": "http://schemas.auth0.com/roles",
  },
}

```

18. Click **Enable**.
19. On the Addon: SAML2 Web App page, click the **Usage** tab.
20. In Identity Provider Metadata, click **Download** and download an XML file with configuration metadata.

You will use this file when configuring an Auth0 SAML provider on Keycloak.

Configuring an Auth0 SAML v2.0 identity provider on Keycloak

About this task

To use Auth0 SSO capabilities and authenticate users, you must configure a SAML v2.0 identity provider on Keycloak.

Before you begin

Configure an application for SSO on Auth0 Dashboard and obtain a configuration metadata file in XML format. For more information, see [Creating a new application](#) on page 110.

Procedure

1. Log in to the Keycloak web administration interface.
2. Navigate to **Solution Realm > Identity Provider**.
3. Click **Add provider** and then select **SAML v2.0**.
Keycloak displays the Add identity provider page.
4. In **Alias**, type the name that you used when configuring an SAML application on Auth0 Dashboard.
For example, Auth0SAML.
5. Navigate to the Import External IDP Config section.
6. Click **Select file**, navigate to the federation metadata XML file that you downloaded from Auth0 and then click **Import**.
Keycloak imports the configuration data and populates the **Single Sign-On Service URL** field.
7. In **NameID Policy Format**, select **Email**.
8. Click **Save**.

Next steps

Configure attribute mapping between Keycloak and the Auth0 identity provider.

Creating users on Auth0

About this task

You must add all your enterprise users who require SSO capabilities to Auth0. When adding a user, you must use the email address configured for this user in your enterprise LDAP.

Procedure

1. Log in to the Auth0 Dashboard as an administrator.
2. Navigate to **User Management > Users**.
3. Click **Create User**.
4. In **Email**, type the user's email address that is configured in your enterprise LDAP.
5. In **Password**, type a password for the user.
6. In **Repeat Password**, re-type the password.
7. In **Connection**, select **Username-Password-Authentication**.
8. Click **Create**.
9. On the Users page, click the user that you have just created.
10. Click the **Details** tab.
11. In the Metadata section, in **user_metadata**, type the following:

```
{
  "family_name": "<lastName>"
  "given_name": "<firstName>"
}
```

In this entry, `<lastName>` is the last name of the user and `firstName` is the first name of the user.

The last name and first name that you provide in **user_metadata** might differ from the values configured for the user in your LDAP.

12. In the Metadata section, in **app_metadata**, type the following:

```
{
  "roles": "<ROLE>"
}
```

In this entry, `<ROLES>` can be one of the following:

- `user`: To add the user to the user group.
- `admin`, To add the user to the administrator group. Select this option if you want to provide administrator rights to the user.

Note:

The SSO capabilities are available to members of both groups.

13. Click **Save**.

Setting up last name and first name attributes in the user's profile

About this task

Auth0 uses the `given_name` and `family_name` attributes to store user's first name and last name respectively. However, you cannot assign values to these attributes directly. You must create a rule that obtains user's first name and last name from the `user_metadata` attribute and assigns the received values to the `given_name` and `family_name` attributes.

For more information about Auth0 rules, see [Auth0 rules](#).

Procedure

1. Log in to the Auth0 Dashboard as an administrator.
2. Navigate to **Auth Pipeline > Rules**.
3. Click **Create**.

Auth0 Dashboard displays the Pick a rule template page.

4. Click **Empty rule**.
5. In **Name**, type a name of your choice for the rule.
6. In **Script**, type the following:

```
function (user, context, callback) {
  if (user.user_metadata.given_name)
    user.given_name = user.user_metadata.given_name;

  if (user.user_metadata.family_name)
    user.family_name = user.user_metadata.family_name;
  callback(null, user, context);
}
```

7. Click **Save changes**.
8. On the Rules page, ensure that the rule that you have just configured is active.

Rules

[+ Create](#)

Custom Javascript snippets that run in a secure, isolated sandbox in the Auth0 service as part of your authentication pipeline. [Learn more](#) ▶

⚠ We recommend you to explore Actions, our newest extensibility product now in General Availability. Actions gives you many of the same functions as Rules and more. Get started today in [Actions](#). [Learn more about Actions](#).

Try all rules with... ▾

🔄 Refresh

Update given-name and family-name from user-metadata



When the rule is active, Auth0 updates the `given_name` and `family_name` attributes whenever you update user's data or create a new user.

Device Authorization flow configuration

The Device Authorization Flow, or device flow, enables clients with limited input capabilities, such as J1XX phones, to use SSO. This flow does not use the embedded Keycloak service and currently supports only the Avaya IAM identity provider. The procedures in this section outline the tasks you must perform to configure the device flow.

Checklist for device flow configuration

The following checklist lists your tasks to configure the device flow on Avaya Aura® Device Services:

No.	Task	Notes	✓
1	Contact Avaya IAM support to configure SSO settings for your enterprise on Avaya IAM. To contact Avaya IAM support: • Submit support request to Avaya IAM (SSO) to integrate with Enterprise IDP. • Upload your Identity Provider (IdP) metadata file using the following link: https://wwwcms.avaya.com/customer/en/home/?modal=show&function=1397208961931&category=1399860014782&mode=direct	To configure the device flow on Avaya Aura® Device Services, you require settings from Avaya IAM.	
2	Ensure that you gathered all the required information.	For information about data required to configure the device flow on Avaya Aura® Device Services, see Prerequisites for Device Authorization Flow configuration on page 54.	
3	If you configure SSO for J1XX phones, publish COMM_ADDR_HANDLE_TYPE and COMM_ADDR_HANDLE_LENGTH parameters.	Avaya Aura® Device Services requires these parameters to provide SIP parameters to J1XX phones automatically. For more information about the publishing process, see Publishing COMM_ADDR_HANDLE parameters for J1XX phones on page 118.	
4	Create client mapping.	See Creating client mapping for the device flow on page 116.	
5	Configure the LDAP UID mapping.	See Configuring the LDAP UID mapping on page 144.	

No.	Task	Notes	✓
6	Synchronize data between Avaya Aura® Device Services and Avaya IAM.	See Synchronizing data between Avaya Aura Device Services and an identity provider on page 145.	
7	Test the integration with Avaya IAM using a physical device.	You <i>cannot</i> test the device flow using the procedure Testing the integration with an identity provider from the Google Chrome web browser on page 146 as it does not support the device flow.	

Creating client mapping for the device flow

About this task

In the device flow, a client mapping contains information that clients use to discover and interact with the Avaya IAM authorization resources.

If you configure SSO for different phones, create separate client mapping for phones with different client IDs. For example, all J1XX phones have the same client ID, aoc-j100-cli. Therefore, you only need a single client mapping for all J1XX phones.

To configure a client mapping for clients that support the Keycloak-based authorization flow, such as Avaya Workplace Client, use the procedure “Create client mapping”.

! Important:

If you have multiple client mappings in your deployment, the value of the Access token email address attribute parameter must be the same for each client mapping.

Before you begin

- Obtain and install the Avaya IAM root CA certificate into the Avaya Aura® Device Services truststore. For more information about adding certificates to truststore, see “Managing truststore certificates”.
- Obtain the Avaya IAM Discovery URL address.
- Ensure that the host name of the Discovery URL is accessible from Avaya Aura® Device Services. If not, obtain a proxy server host name from your identity provider and ensure that this host name is accessible from Avaya Aura® Device Services.
- Obtain the client ID for your phone from Avaya support.
- If you already have another client mapping on Avaya Aura® Device Services, record the value of the **Access token email address attribute** parameter configured for that client mapping. For more information about reviewing client mapping settings, see “Managing an existing client mapping”.

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal with the Security administrator role.
2. Navigate to **Security Settings > Client ID Mapping**.

3. Click **Add**.
4. In the Create new client mapping window, complete the following fields:
 - a. In **Client ID**, type the client ID of the phone series.
For example, for J1xx phones, type `aoc-j100-cli`. This value is case-sensitive.
 - b. In **OIDC Discovery URL**, type the Avaya IAM Discovery URL address.
 - c. In **Client Secret**, type one of the following:
 - If Avaya IAM configures your phones as “public”, type `NA`.
 - If Avaya IAM configures your phones as “private”, type the client secret that Avaya IAM provides.
 - d. Configure **Proxy Address** as the following:
 - If the host name of the Discover URL is accessible from Avaya Aura® Device Services, keep the field blank.
 - If the host name of the Discovery URL is not accessible from Avaya Aura® Device Services, type the host name of the proxy server that Avaya IAM provides.
 - e. In **Client Name**, type the client name configured on Avaya IAM for your organization.
 - f. Select the **Enable device Auth** check box.

 Note:

Client name field must be provided if the **Enable device auth** field is checked and the client name must start with `aads-`.

For upgrading to AADS 10.2, post installation, you must update the client name for the already present data.

Do not add or update **Client name** field for client versions 4.1.2.0 and below.

5. Click **OK**.
Avaya Aura® Device Services displays the new client mapping on the page.
6. If you already have another client mapping in your deployment, do the following:
 - a. On the Client ID Mapping page, click **Edit** for the client mapping you have just created.
 - b. Ensure that the value of the **Access token email address attribute** matches the value that you recorded.
 - c. If the values are different, update the **Access token email address attribute** with the value that you recorded.
 - d. Click **OK**.

Related links

[Managing truststore certificates](#) on page 233

[Creating client mapping](#) on page 126

[Managing an existing client mapping](#) on page 128

Publishing COMM_ADDR_HANDLE parameters for J1XX phones

About this task

To enable Avaya Aura® Device Services to automatically provide J1XX phones with SIP parameters, such as SIPDOMAIN or SIP_CONTROLLER_LIST, configure the following parameters using the Dynamic Configuration Service:

- COMM_ADDR_HANDLE_TYPE
- COMM_ADDR_HANDLE_LENGTH

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal.
2. Navigate to **Dynamic Configuration > Configuration**.
3. On the Configuration page, click the **Global** tab.
4. In **COMM_ADDR_HANDLE_TYPE**, select *Avaya SIP*.
5. In **COMM_ADDR_HANDLE_LENGTH**, type the number of digits in extension numbers in your enterprise.
6. Click **Save**.
7. In the Save Configuration window, select **Overwrite existing configuration** and select an existing configuration.
8. Click **Publish**.
The web administration portal displays the Publish/Delete Settings dialog box.
9. Select the **Global settings will be applied to all users** check box.
10. Click **Publish**.
11. In the confirmation window, click **Yes**.

Workspaces SSO Flow configuration

The Workspaces SSO Flow, enables users to use their organization credentials to log in to Avaya Workspaces, and use AADS search APIs. This flow does not use the Keycloak service embedded in AADS. It leverages Identity and Access Management (IAM) for agent authentication and authorization. The procedures in this section outline the tasks you must perform to configure the Workspaces SSO Flow.

Related links

[Prerequisites for Workspaces SSO configuration](#) on page 54

Checklist for Workspaces SSO Flow configuration

The following checklist lists your tasks to configure the Workspaces SSO Flow on Avaya Aura® Device Services:

No.	Task	Notes	✓
1	Ensure that you gathered all the required information.	For information about data required to configure the Workspaces SSO Flow on Avaya Aura® Device Services, see Prerequisites for Workspaces SSO configuration on page 54.	
2	Create client mapping.	See Creating client mapping for the Workspaces SSO Flow on page 119.	
3	Configure the LDAP UID mapping.	See Configuring the LDAP UID mapping on page 144.	

! Important:

You *cannot* test the Workspaces SSO Flow using the procedure [Testing the integration with the identity provider from the web administration portal](#) on page 147.

Creating client mapping for the Workspaces SSO Flow

About this task

In the Workspaces SSO Flow, a client mapping contains information that clients use to discover and interact with the Identity and Access Management (IAM) authorization resources.

To create client mapping, see “Create client mapping”.

! Important:

If you have multiple client mappings in your deployment, the value of the Access token email address attribute parameter must be the same for each client mapping.

Before you begin

- Obtain the OIDC URL for IAM service, which is the discovery URL of the IAM service.
- Ensure that the hostname of the discovery URL is accessible from Avaya Aura® Device Services. If not, obtain a proxy server hostname from the IAM service and ensure that it is accessible from Avaya Aura® Device Services.
- Obtain the client name, which is the name of the client configured on the IAM service.
- Obtain the client ID, which can be any unique identifier configured for the client.
- If you already have another client mapping on Avaya Aura® Device Services, record the value in the **Access token email address attribute** field configured for that client mapping. For more information about reviewing client mapping settings, see “Managing an existing client mapping”.

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal with the Security administrator role.
2. Navigate to **Security Settings > Client ID Mapping**.
3. Click **Add**.
4. On the Create new client mapping window, complete the following fields:
 - a. In the **Client ID** field, type the client ID.
This value is case-sensitive.
 - b. In the **OIDC Discovery URL** field, type the discovery URL of the IAM service.
 - c. In the **Client Secret** field, type NA.
 - d. Configure **Proxy Address** as the following:
 - If the hostname of the discovery URL is accessible from Avaya Aura® Device Services, keep the field blank.
 - If the hostname of the discovery URL is not accessible from Avaya Aura® Device Services, type the hostname of the proxy server for the IAM service.
 - e. In the **Client Name** field, type the client name configured on the IAM service.
5. Click **OK**.
Avaya Aura® Device Services displays the new client mapping on the page.
6. If you already have another client mapping in your deployment, do the following:
 - a. On the Client ID Mapping page, click **Edit** for the newly created client mapping.
 - b. Ensure that the value in the **Access token email address attribute** field matches the value on the other client mapping.
 - c. If the values are different, update the value in the **Access token email address attribute** field with the value on the other client mapping.
 - d. Click **OK**.

Related links

[Creating client mapping](#) on page 126

[Managing an existing client mapping](#) on page 128

Switching to another identity provider

Avaya Aura® Device Services supports the simultaneous use of multiple identity providers. If you want to use multiple identity providers, you only need to configure integration with the new identity provider. However, if you want to switch from one identity provider to another, you must perform additional tasks on Keycloak. The procedures in this section outline the tasks you must perform to switch to another identity provider.

Checklist for switching to another identity provider

The following checklist lists the configuration tasks you must perform to switch to another identity provider.

No.	Task	Notes	✓
1	Delete the existing users from Keycloak.	See Deleting users from Keycloak on page 121.	
2	Configure integration with the new identity provider.	See the configuration checklist for the appropriate identity provider.	
3	Disable the previously configured identity provider.	See Disabling an identity provider on page 121.	
4	Change the identity provider redirector.	See Changing the identity provider redirector on page 122.	

Deleting users from Keycloak

About this task

If you switch to another identity provider, you must delete from Keycloak all users you configured for the previous identity provider.

Keycloak does not support deleting users in bulk. You must delete users manually one by one.

Procedure

1. On the Keycloak web administration interface, navigate to your realm.
2. In the Manage area, click **Users**.
3. On the Users page, click **View all users**.
4. To delete a user from Keycloak, in the rightmost column, click **Delete** for the user.
5. Repeat the previous steps for all remaining users on Keycloak.

Disabling an identity provider

About this task

If you do not want to use an identity provider, you can disable it. Keycloak stores the identity provider configuration, so you can enable it later, if required.

Procedure

1. On the Keycloak web administration interface, navigate to your realm and then click **Identity Providers**.
2. Select your identity provider.
3. Switch **Enabled** to **Off**.
4. Click **Save**.

Changing the identity provider redirector

About this task

After configuring the new identity provider settings, configure the Keycloak identity provider redirector to use this identity provider in the authentication flow.

Before you begin

Procedure

1. On the Keycloak web administration interface, navigate to your realm and then click **Identity Providers**.
2. Copy the name of your new identity provider.
3. Navigate to **Authentication > Flows**.
4. From the drop-down list, select **Browser**.
5. In the table, in the Identity Provider Redirector row, click **Actions** and then select **Config**.
6. To delete the current configuration, click **Delete** (trash icon).
7. Click **Actions** and then select **Config**.
8. In **Alias** and **Default identity**, paste the identity provider name that you copied in step 2.
9. Click **Save**.

Logging in to the Keycloak web administration portal

About this task

Use this procedure to log in to the Keycloak web administration portal. The portal becomes available after you configure Keycloak settings during the initial Avaya Aura® Device Services configuration.

For more information about installation and initial configuration, see *Deploying Avaya Aura® Device Services*.

Procedure

1. Open a web browser.
2. Enter the following URL:
`https://<AADS IP or FQDN>:8445/auth/admin`
In this URL, <AADS IP or FQDN> is either the Avaya Aura® Device Services front-end FQDN or IP address.
3. Enter the user name and the password that you created when configuring the Keycloak settings.

For more information, see “Configuring Keycloak settings”.

Changing your Keycloak password

About this task

From the Avaya Aura® Device Services configuration utility, you can change the password that you use to access the Keycloak web administration portal. The new password must comply with the password complexity rules.

Procedure

1. Log in to the Avaya Aura® Device Services seed node as an administrator.
2. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.
3. Select **Keycloak Configuration**.
4. In **Keycloak Admin user**, type the user name of the Keycloak administrator for which you want to change the password.
5. In **Keycloak Admin user's password**, type a new password.
6. In **Update Keycloak Admin user's password**, type `y`.
7. In **Keycloak Admin user's current password**, type the current password.
8. In **Keycloak Admin user's new password**, re-type the new password.
9. Confirm the new password.
10. Select **Apply**.
11. Select **Continue**.

Related links

[passwdrules command](#) on page 458

[Characters supported for Avaya Aura Device Services passwords](#) on page 323

Authorization realm configuration on UC servers and Avaya Workplace Client

When SSO/OAuth is enabled on Avaya Aura® Device Services, you must provision the following parameters for all Avaya Workplace Client softphones configured to use the Avaya Authorization service (OAuth2):

- **AVAYA_AUTHORIZATION_REALM**: Set the value to the Keycloak realm configured on Avaya Aura® Device Services, which is "SolutionRealm" by default.

Important:

If other UC servers, such as Avaya Aura® Web Gateway or Presence and Multimedia Messaging, are configured to use SSO/OAuth, ensure that they use the same Keycloak realm.

- ACSSSO: Set the value to 3, so that Avaya Workplace Client uses Avaya Authorization for Avaya Aura® Device Services.
- ESMSSO: Set the value to 3, so that Avaya Workplace Client uses Avaya Authorization for Presence and Multimedia Messaging.
- AUTOCONFIG_USESSO: Set the value to 3 so that Avaya Workplace Client uses Avaya Authorization for automatic configuration.
- SETTINGS_FILE_URL: Set the value to the Avaya Aura® Device Services dynamic configuration URL with the additional `preferredAuth=bearer` query parameter.
For example: `https://<AADS_FRONT_END_FQDN>:<AADS_PORT>/acs/resources/configurations?preferredAuth=bearer`

 Note:

In a cluster environment, if you use front-end port 443, you must use the Avaya Aura® Device Services front-end FQDN or virtual IP address when configuring this parameter.

Configuring Keycloak settings

About this task

Use this procedure to set up a Keycloak administrator account. Avaya Aura® Device Services configures Keycloak automatically. After the configuration process is complete, you can view and update the default configuration using the Keycloak web administration portal.

If you use the Shibboleth identity provider, you can also upload an identity provider entity descriptor file in XML format.

 Important:

You can upload an entity descriptor file using the Avaya Aura® Device Services configuration utility for the Shibboleth identity provider only. For other identity providers, you must upload an entity descriptor file using the Keycloak web administration portal. If you do not upload an entity descriptor file to Keycloak, OAuth will not work.

Before you begin

- Install Avaya Aura® Device Services.
- Ensure that you gather all information and configured an SSO application on the third-party identity provider. For information about the prerequisites, see [Prerequisites for SSO configuration](#) on page 52.
- If you configure the Shibboleth identity provider, obtain the IDPSSODescriptor configuration file in the XML format. You can download the file from `https://<shibboleth site address>:<port>/idp/shibboleth`.

Procedure

1. On the seed node, run the Avaya Aura® Device Services configuration utility using the `app configure` command.

2. Select **Keycloak Configuration**.
3. In the **Keycloak Admin** and **Keycloak Admin user's password** fields, provide a user name and password of your choice for the initial Keycloak administrative account.

These credentials are used to log in to the Keycloak web administration portal. Your password must comply with the password complexity rules.
4. **(Optional)** If you are configuring the Shibboleth identity provider, do the following to upload the identity provider configuration file:
 - a. Upload the identity provider configuration file to the seed node using a file transfer program, such as SFTP or SCP.
 - b. In the **IDP XML** field, enter `y`.
 - c. In the **Custom IDP xml file** field, select the IPDSSODescriptor configuration file that you uploaded to Avaya Aura® Device Services.

If you do not provide the Shibboleth configuration file using CLI, you must upload this file later using the Keycloak administration portal.

5. If you want to configure the mapping between attributes used by the identity provider and attributes used by Keycloak, do the following:
 - a. In **Last Name attribute**, provide the Last Name attribute that is used by the identity provider. For example, `sn`.
 - b. In **First Name attribute**, provide the First Name attribute that is used by the identity provider. For example, `givenName`.
 - c. In **Membership attribute**, provide the Membership attribute containing role information that is used by the identity provider. For example, `memberOf`.
 - d. In **User Role value**, provide the User Role value, which comes from the Membership attribute. It must be a full LDAP distinguished name (DN). For example, `cn=users,dc=avaya,dc=com`.
 - e. In **Administrator Role value**, provide the Administrator Role value, which comes from the Membership attribute. It must be a full LDAP DN. For example, `cn=admins,dc=avaya,dc=com`.

You can configure the mapping later using the Keycloak administration portal.

6. Select **Apply**.
7. After the configuration process is complete, select **Continue**.

Next steps

If required, view and configure additional Keycloak settings using the Keycloak web administration portal. For more information, see “Logging in to the Keycloak web administration portal” in *Administering Avaya Aura® Device Services*.

Related links

[passwdrules command](#) on page 458

Starting and stopping the Keycloak service

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run one of the following commands:
 - `svc keycloak start` to start the Keycloak service.
 - `svc keycloak stop` to stop the Keycloak service.
 - `svc keycloak restart` to restart the Keycloak service.

Obtaining the client secret

About this task

The client secret is required to establish communication between Keycloak and Avaya Aura® Device Services. The client secret is generated automatically during Keycloak configuration.

Procedure

1. On the Keycloak web administration portal, navigate to your realm and then click **Clients**.
By default, the realm is SolutionRealm.
2. From the Clients table, select **aads**.
3. Click the **Credentials** tab.
4. Copy the text in **Secret** field.

Next steps

Create a client mapping as described in [Creating client mapping](#) on page 126.

Creating client mapping

About this task

In the authorization flow, Avaya Aura® Device Services interacts with Keycloak on behalf of a client, such as Avaya Workplace Client, Avaya Meeting Scheduler Outlook Add-in, Avaya Meetings Server Unified Portal, Avaya Agent for Desktop, or Avaya Calling for Microsoft Teams. To enable Avaya Aura® Device Services to communicate with Keycloak, you must provision Avaya Aura® Device Services with the Keycloak client secret and the URL to discover Keycloak resources. You must create a client mapping for each client that your deployment supports.

! Important:

If you have multiple client mappings in your deployment, the value of Access token email address attribute must be the same for each client mapping.

To configure the device flow for phones, such as J1XX, see “Creating client mapping for the device flow” in *Administering Avaya Aura® Device Services*.

Before you begin

- Obtain the client secret as described in [Obtaining the client secret](#) on page 126.
- If you already have another client mapping on Avaya Aura® Device Services, record the value of **Access token email address attribute** configured for that client mapping. For more information, see [Managing an existing client mapping](#) on page 128.

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal with the Security administrator role.
2. Navigate to **Security Settings > Client ID Mapping**.
3. Click **Add**.
4. In the Create new client mapping window, complete the fields as follows:

- a. In **Client ID**:

- For Avaya Workplace Client, type `Equinox`.
- For Avaya Meeting Scheduler Outlook Add-in, type `MeetingScheduler`.
- For Avaya Meetings Server Unified Portal, type `UnifiedPortal`.
- For Avaya Agent for Desktop, type `aafd`.
- For Avaya Calling for Microsoft Teams, type `CallAssist`.

This value is case sensitive.

- b. In **OIDC Discovery URL**, type `https://<AADS_FQDN>:<PORT>/auth/realms/<REALM>/ .well-known/openid-configuration`

In this string:

- `<AADS_FQDN>` is the Avaya Aura® Device Services front-end FQDN.
- `<PORT>` is the Avaya Aura® Device Services front-end FQDN service port.
- `<REALM>` is the Keycloak realm, which is `SolutionRealm` by default.

- c. In **Client Secret**, enter the string copied from the Keycloak web administration interface.
- d. Leave the **Client Name** and **Proxy Address** fields blank.
- e. Clear the **Enable device Auth** check box.
- f. For other fields, keep the default values.

5. Click **OK**.

Avaya Aura® Device Services displays the new client mapping on the page.

6. If you already have another client mapping in your deployment, do the following:
 - a. On the Client ID Mapping page, click **Edit** for the client mapping that you have just created.
 - b. Ensure that the value of **Access token email address attribute** matches the value that you recorded.
 - c. If the values are different, update **Access token email address attribute** with the value that you recorded.
 - d. Click **OK**.
7. **(Optional)** Create a client mapping for any additional clients that your deployment supports.

Related links

[Creating client mapping for the device flow](#) on page 116

[Creating client mapping for the Workspaces SSO Flow](#) on page 119

[Managing an existing client mapping](#) on page 128

Managing an existing client mapping

About this task

Use this procedure to review or edit identity provider mapping settings.

Caution:

Do *not* use this procedure for updating public keys of a client mapping. To update public keys, synchronize data with the identity provider as described in “Synchronizing data between Avaya Aura® Device Services and an identity provider”.

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal with the Security administrator role.
2. Navigate to **Security Settings > Client ID Mapping**.
3. Select the required client mapping and then click **Edit**.
4. Update the settings as required.
5. Click **OK**.

Configuring a time interval for updating public keys in client mappings

About this task

By default, Avaya Aura® Device Services automatically updates public keys used in client mappings every 24 hours. You can update this interval as appropriate by configuring system properties in the `catalina.properties` file.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as the root user.
2. To open the `catalina.properties` file in the vi editor, run the following commands:

```
cdto active
vi tomcat/<tomcat_version>/conf/catalina.properties
```

3. Add the following entry to the file:

```
com.avaya.cas.oauth.keyupdate.interval=<TIME_IN_SECONDS>
```

In this entry, `<TIME_IN_SECONDS>` is the interval between two consecutive attempts to update public keys in seconds. For example, to update public keys weekly, set the property to 604800 as follows:

```
com.avaya.cas.oauth.keyupdate.interval=604800
```

4. Save the file.
5. Run the following command to restart Tomcat and apply the changes:

```
svc tomcat restart
```

Regenerating the Keycloak client secret

About this task

Use this procedure if you need to regenerate a new Keycloak client secret. For example, this is useful if your company requires you to change your password periodically.

Procedure

1. On the Keycloak web administration interface, navigate to your realm and then click **Clients**.

The default realm created by Avaya Aura® Device Services is "SolutionRealm".

2. From the Clients table, select **aads**.
3. Click the **Credentials** tab.
4. Click **Regenerate Secret**.

Next steps

Update the identity provider to client mapping.

Related links

[Updating the identity provider mapping](#) on page 130

Updating the identity provider mapping

About this task

Use this procedure to review or edit identity provider mapping settings. You must update the mapping after regenerating the Keycloak client secret.

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal with the Security administrator role.
2. Navigate to **Security Settings > Client ID Mapping**.
3. Select a client mapping configuration.
4. Click **Edit**.
5. Update the fields as required.
6. Click **OK**.

Importing third-party identity provider private CA certificates

About this task

If you integrate Avaya Aura® Device Services with a third-party identity provider that is using a private CA, you must import the private CA certificates into the Java truststore. This allows you to import the third-party identity provider configuration XML file directly from the identity provider.

In cluster deployments, perform this procedure on the seed node first and then on all non-seed nodes.

If you redeploy the virtual machines, you must perform this procedure again.

Before you begin

Obtain the root and, if required, intermediate CA certificates in PEM format for the CA that signs the provider's identity certificate.

Procedure

1. Transfer the CA certificates to the Avaya Aura® Device Services node using a file transfer program, such as SFTP or SCP.
2. Log in to the Avaya Aura® Device Services node using an SSH connection.

3. Navigate to `/etc/pki/java`.

4. Run the following command to import the root certificate into the truststore:

```
sudo keytool -importcert -keystore ./cacerts -alias idpca -file
<PATH>
```

In this command, `<PATH>` is the full path to the CA certificate in PEM format.

 Note:

The keystore password is `changeit`.

5. Repeat the previous step for all required intermediate CA certificates.

Importing a third-party identity provider

About this task

To use SSO capabilities and authenticate users, you must import a third-party identity provider.

Use this procedure if you want to import the provider using the Keycloak web administration portal. You can also import a third-party identity provider using the Avaya Aura® Device Services configuration utility as described in *Deploying Avaya Aura® Device Services*.

Before you begin

- Obtain the identity provider configuration file in XML format from the provider.
- If the identity provider uses a certificate signed by a private CA, you must import the CA certificate chain for the identity provider to the default Java truststore. For more information, see [Importing third-party identity provider private CA certificates](#) on page 130.

Procedure

1. On the Keycloak web administration interface, navigate to your realm and then click **Identity Providers**.

2. Click **Add provider** and then select **SAML v2.0**.

3. In the **Alias** field, enter a name of your choice.

For example: `Shibboleth`

Other fields are optional.

4. To import configuration data from the identity provider configuration file, do one of the following:

- To upload the configuration file downloaded from the provider, click **Select file** and then select the configuration file that is stored on your computer.
- To upload the configuration file directly from the provider, in the **Import from URL**, enter the configuration file URL.

For example, for Shibboleth, the URL is `https://<shibboleth site address>:<port>/idp/shibboleth`

Keycloak imports the configuration data and populates the **Single Sign-On Service URL** field.

5. Click **Save**.

Next steps

Select the identity provider.

Related links

[Selecting the default identity provider](#) on page 132

Selecting the default identity provider

About this task

When you select a default identity provider, Keycloak redirects Avaya Workplace Client users directly to the selected identity provider instead of displaying the login screen first.

If you have a single identity provider configured, use this procedure if you configured the provider using the Keycloak web administration portal. If you configured the identity provider using the configuration utility, the provider is already selected.

If you have multiple identity providers configured, you can select which identity provider you want to use for authorization. Otherwise, Keycloak will prompt Avaya Workplace Client users to select an identity provider to authenticate.

* Note:

Do not select the default identity provider if you want to enable the simultaneous use of multiple identity providers for Avaya Workplace Client users.

Before you begin

Configure the required identity provider on Keycloak.

Procedure

1. On the Keycloak web administration portal, navigate to your realm and then click **Authentication**.
2. Click the **Flows** tab.
3. From the drop-down list, select **Browser**.
4. In the Identity Provider Redirector row, click **Actions** and then select **Config**.

Avaya Aura® Device Services displays the Create authenticator configuration window.

5. In the **Alias** field, enter a name of your choice.

For example: `Shibboleth`.

6. In the **Default Identity Provider**, enter the alias of the configured identity provider for OAuth.

Disabling the default identity provider

About this task

If you plan to use multiple identity providers simultaneously, you must disable the default identity provider. When the default identity provider is disabled, Keycloak prompts Avaya Workplace Client to select an identity provider to authenticate.

Procedure

1. On the Keycloak web administration portal, navigate to your realm and then click **Authentication**.
2. Click the **Flows** tab.
3. From the drop-down list, select **Browser**.
4. In the table, in the Identity Provider Redirector row, click **Actions** and then select **Config**.
Avaya Aura® Device Services displays the Create authenticator configuration window.
5. Clear the **Default Identity Provider** field.
6. Click **Save**.

Modifying the attribute mapping between the third-party identity provider and Keycloak

About this task

To authenticate a user, a third-party identity provider sends to Keycloak an authentication response that contains various user attributes, such as first name, last name, phone number, and email address. Keycloak then maps this user information to the attributes of the access token that is generated and sent back to clients.

The Avaya Aura® Device Services configuration utility provides a default attribute mapping. The identity provider you are using, however, might use attribute names that differ from the attribute names provided in the default mapping. In this case, you must update the default mapping. Use this procedure to modify the default attribute mapping.

Important:

You can only configure a single mapper of the “Role Mapper” category for an identity provider. Keycloak does not support multiple Role Mappers.

Depending on the identity provider that you are using, you must configure the mappers as follows:

- For the Microsoft Azure Active Directory SAML v2.0 identity provider, configure the mappers listed in [Attribute mapping parameters for Microsoft Azure SAML v2.0 identity provider](#) on page 136.
- For the Microsoft Office 365 OAuth2 identity provider, configure the mappers listed in [Attribute mapping parameters for Office 365 OAuth2 identity provider](#) on page 136.
- For the Ping Identity SAML v2.0 identity provider, configure the mappers listed in [Attribute mapping parameters for Ping Identity SAML v2.0 identity provider](#) on page 137.
- For the OKTA SAML v2.0 identity provider, you must configure the mappers listed in [Attribute mapping parameters for OKTA SAML v2.0 identity provider](#) on page 138.
- For the AD FS SAML v2.0 identity provider, you must configure the mappers listed in [Attribute mapping parameters for ADFS SAML v2.0 identity provider](#) on page 138.
- For the OneLogin SAML v2.0 identity provider, you must configure the mappers listed in [Attribute mapping parameters for OneLogin SAML v2.0 identity provider](#) on page 139.
- For the IBM SAML v2.0 identity provider, you must configure the mappers listed in [Attribute mapping parameters for the IBM SVA SAML v2.0 identity provider](#) on page 139.
- For the Duo SAML v2.0 identity provider, you must configure the mappers listed in [Attribute mapping parameters for the Duo SAML v2.0 identity provider](#) on page 140.
- For the Imprivata SAML v2.0 identity provider, you must configure the mappers listed in [Attribute mapping parameters for Imprivata SAML v2.0 identity provider](#) on page 141.

Before you begin

Configure a third-party identity provider on Keycloak.

Procedure

1. On the Keycloak web administration portal, navigate to your realm and then click **Identity Providers**.
2. Select the identity provider.
3. Click **Mappers**.
4. From the table, select an appropriate attribute.

Avaya Aura® Device Services displays the attribute mapping for the selected attribute.

- The **Friendly Name** field contains the attribute name that the identity provider passes to Keycloak.

If the identity provider does not provide a value for the **Friendly Name** field, use the **Attribute Name** field instead.

- The **User Attribute Name** field contains the attribute name that Keycloak passes to clients in access tokens.

For a person's given name, last name, and email address, use the following **User Attribute Name** values:

- Given name: `givenName`.

- Last name: `lastName`.
- Email address: `email`

These values are case sensitive.

The following image shows the `givenName` attribute.

The screenshot shows the 'GivenName' mapper configuration in Keycloak. The breadcrumb trail is 'Identity Providers > saml > Identity Provider Mappers > GivenName'. The form includes fields for ID (1cb82654-acb7-449b-8e35-2d82d5b07cd7), Name (givenName), Mapper Type (Attribute Importer), Attribute Name (empty), Friendly Name (givenName), and User Attribute Name (firstName). There are 'Save' and 'Cancel' buttons at the bottom.

5. Modify the **Friendly Name** value according to the attribute name that is used by the identity provider you are using.
6. If **Mapper type** is set to **SAML Attribute to Role**, do the following to map a role:
 - a. Click **Select Role**.
 - b. In the Role Selector window, in the **Client Roles** drop-down list, select **aads**.
 - c. Select the required role and then click **Select client role**.

The screenshot shows the 'Aads.user' mapper configuration in Keycloak. The breadcrumb trail is 'Identity Providers > Shibboleth > Identity Provider Mappers > Aads.user'. The form includes fields for ID (a35bddcc-efa0-4d33-978d-888a7322cf77), Name (aads.user), Mapper Type (SAML Attribute to Role), Attribute Name (empty), Friendly Name (memberOf), Attribute Value (UCUser), and Role (aads.user). There is a 'Select Role' button next to the Role field, and 'Save' and 'Cancel' buttons at the bottom.

7. Click **Save**.
8. Repeat the above steps for any other attributes you need to map.

Attribute mapping parameters for Office 365 OAuth2 identity provider

The following table lists mappers that you must configure if you are using Office 365 OAuth2 identity provider:

Mapper name	Mapper type	Attribute name	User Attribute Name	Role
user.groups	Hardcoded Role	—	—	aads.user
givenname	Attribute Importer	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	firstName	—
surname	Attribute Importer	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	lastName	—
emailaddress	Attribute Importer	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	email	—

The following image shows the emailaddress mapper configuration:

The screenshot shows the configuration form for the 'Emailaddress' mapper. The fields are as follows:

- ID:** b4580f27-0e95-440a-95e2-0a7ff3a0220a
- Name:** emailaddress
- Mapper Type:** Attribute Importer
- Attribute Name:** http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
- Friendly Name:** (empty)
- User Attribute Name:** email

At the bottom of the form are 'Save' and 'Cancel' buttons.

Attribute mapping parameters for Microsoft Azure SAML v2.0 identity provider

The following table lists mappers that you must configure if you are using the Microsoft Azure SAML v2.0 identity provider:

Mapper name	Mapper type	User Attribute Name	Attribute Name	Attribute Value	Role
firstName	Attribute Importer	firstName	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	firstName	—
lastName	Attribute Importer	lastName	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	lastName	—
email	Attribute Importer	email	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	email	—
aads.user	SAML Attribute to Role	—	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	The ID of the User Group configured on Microsoft Azure	aads.user
aads.admin	SAML Attribute to Role	—	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	The ID of the Administrator group configured on Microsoft Azure	aads.admin

Attribute mapping parameters for Ping Identity SAML v2.0 identity provider

The following table lists mappers that you must configure if you are using the Ping Identity SAML v2.0 identity provider:

Mapper name	Mapper Type	Attribute Name	User Attribute Name	Attribute Value	Role
firstName	Attribute Importer	firstName	firstName	—	—
lastName	Attribute Importer	lastName	lastName	—	—
email	Attribute Importer	email	email	—	—
aads.user	SAML Attribute to Role	Group	—	The ID of the Population user group configured on Ping Identity	aads.user

Mapper name	Mapper Type	Attribute Name	User Attribute Name	Attribute Value	Role
aads.admin	SAML Attribute to Role	Group	—	The ID of the Population administrator group configured on Ping Identity	aads.admin

Attribute mapping parameters for OKTA SAML v2.0 identity provider

The following table lists mappers that you must configure if you are using the OKTA SAML v2.0 identity provider:

Mapper name	Mapper Type	Attribute Name	User Attribute Name	Attribute Value	Role
firstName	Attribute Importer	firstName	firstName	—	—
lastName	Attribute Importer	lastName	lastName	—	—
email	Attribute Importer	email	email	—	—
aads.user	SAML Attribute to Role	User	—	The name of the user group configured on OKTA	aads.user
aads.admin	SAML Attribute to Role	Admin	—	The name of the administrator group configured on OKTA	aads.admin

Attribute mapping parameters for ADFS SAML v2.0 identity provider

The following table lists mappers that you must configure if you are using the ADFS SAML v2.0 identity provider:

Mapper name	Mapper Type	Attribute Name	User Attribute Name	Attribute Value	Role
givenname	Attribute Importer	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	firstName	—	—

Mapper name	Mapper Type	Attribute Name	User Attribute Name	Attribute Value	Role
surname	Attribute Importer	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	lastName	—	—
emailaddress	Attribute Importer	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	emailaddress	—	—
aads.user	SAML Attribute to Role	http://schemas.xmlsoap.org/claims/Group	—	The name of the user group configured on ADFS	aads.user
aads.admin	SAML Attribute to Role	http://schemas.xmlsoap.org/claims/Group	—	The name of the administrator group configured on ADFS	aads.admin

Attribute mapping parameters for OneLogin SAML v2.0 identity provider

The following table lists mappers that you must configure if you are using the OneLogin SAML v2.0 identity provider:

Mapper name	Mapper Type	Attribute Name	User Attribute Name	Attribute Value	Role
firstName	Attribute Importer	firstName	firstName	—	—
lastName	Attribute Importer	lastName	lastName	—	—
email	Attribute Importer	email	email	—	—
aads.user	SAML Attribute to Role	Group	—	user	aads.user
aads.admin	SAML Attribute to Role	Group	—	admin	aads.admin

Attribute mapping parameters for the IBM SVA SAML v2.0 identity provider

The following table lists mappers that you must configure if you are using the IBM SVA SAML v2.0 identity provider:

Mapper name	Mapper Type	Attribute Name	User Attribute Name	Attribute Value	Role
firstName	Attribute Importer	firstName	firstName	—	—
lastName	Attribute Importer	lastName	lastName	—	—
email	Attribute Importer	email	email	—	—
aads.user	SAML Attribute to Role	groupIds	—	The name of the user group configured on IBM SVA	aads.user
aads.admin	SAML Attribute to Role	groupIds	—	The name of the administrator group configured on IBM SVA	aads.admin

Attribute mapping parameters for the Duo SAML v2.0 identity provider

The mapping attributes for the Duo SAML v2.0 identity provider depend on the authentication source that you configured on DAG. The following table lists mappers that you must configure if you are using the Active Directory as the authentication source:

Mapper name	Mapper Type	Attribute Name	User Attribute Name	Attribute Value	Role
firstName	Attribute Importer	givenName This is the first name attribute of your authentication source.	firstName	—	—
lastName	Attribute Importer	sn This is the last name attribute of your authentication source.	lastName	—	—
email	Attribute Importer	mail This is the email attribute of your authentication source.	email	—	—
aads.user	SAML Attribute to Role	memberOf This is the group attribute of your authentication source.	—	The name of the LDAP user group in the Active Directory. For example: CN=user,OU=Roles,DC=aam1,DC=com	aads.user

Mapper name	Mapper Type	Attribute Name	User Attribute Name	Attribute Value	Role
aads.admin	SAML Attribute to Role	memberOf This is the group attribute of your authentication source.	—	The name of the LDAP administration group in the Active Directory. For example: CN=Admin,OU=Roles,DC=aam1,DC=com	aads.admin

If you are using other authentication sources, you must configure the “Attribute Name”, “User Attribute Name”, and “Attribute Value” parameters according to your authentication source attributes. For information about other authentication sources, see the Duo documentation at <https://duo.com/docs/dag>.

Attribute mapping parameters for Imprivata SAML v2.0 identity provider

The following table lists mappers that you must configure if you are using the Imprivata SAML v2.0 identity provider:

Mapper name	Mapper Type	Attribute Name	User Attribute Name	Attribute Value	Role
firstName	Attribute Importer	firstName	firstName	—	—
lastName	Attribute Importer	lastName	lastName	—	—
aads.user	SAML Attribute to Role	memberOf This is the group attribute of your LDAP.	—	The name of the user group configured in your LDAP. For example: CN=User,DC=aam1,DC=com	aads.user
aads.admin	SAML Attribute to Role	memberOf This is the group attribute of your LDAP.	—	The name of the administration group in your LDAP. For example: CN=Admin,DC=aam1,DC=com	aads.admin

Attribute mapping parameters for Auth0 SAML v2.0 identity provider

The following table lists mappers that you must configure if you are using the Auth0 SAML v2.0 identity provider:

Mapper name	Mapper type	User Attribute Name	Attribute Name	Role
firstName	Attribute Importer	firstName	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	—
lastName	Attribute Importer	lastName	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	—
email	Attribute Importer	email	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	—
aads.user	SAML Attribute to Role	user	http://schemas.auth0.com/roles	aads.user
aads.admin	SAML Attribute to Role	admin	http://schemas.auth0.com/roles	aads.admin

Checklist to Configure Keycloak using a secure LDAP

Configuration Checklist

The following checklist outlines the configuration tasks that you must perform:

No.	Task	Notes	✓
1	Obtain LDAP server certificate	Obtaining LDAP Server Certificate on page 142	
2	Import the certificate to a keycloak Truststore	Importing the Certificate into the Keycloak Truststore on page 143	
3	Configure LDAPS in Keycloak	Configuring LDAPS in Keycloak on page 144	

Obtaining LDAP Server Certificate

About this task

Use this procedure to obtain LDAP server certificate and configure Keycloak using a secure LDAP.

Before you begin

Use `openssl` to export the LDAP server's certificate, by running the following commands:

```
echo | openssl s_client -connect <LDAP FQDN>:636 -showcerts
```

```
echo | openssl s_client -connect ldap.example.com:636 -showcerts
```

Example:

The following command displays the LDAP servers certificate:

```
echo | openssl s_client -connect
asewinsrvdc.aseteam.ch:636 -showcerts
```

- When the certificate is displayed, copy the certificate along with the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines to a file. For example: ldap-server.crt.

Next steps

Importing the Certificate into the Keycloak Truststore

Importing the Certificate into the Keycloak Truststore

About this task

If your Keycloak installation uses a Java keystore, you must first convert the certificate to the JKS format and then import it into a Java Keystore (JKS) file. To import the certificate into a Keycloak truststore, you must use the truststore used by the Java runtime Keycloak.

Procedure

1. Run the following command to import the certificate into a Java Keystore (JKS) file:

```
keytool -import -alias ldap-server -file ldap-server.crt -keystore
truststore.jks -storepass changeit
```

Example:

```
keytool -import -alias ldap-server -file /home/admin/ldap-
server.crt -keystore truststore.jks -storepass changeit
```

2. Run the following command to import the certificate into the Keycloak Truststore:

```
keytool -importcert -file ldap-server.crt -alias ldap-server
-keystore /path/to/keycloak/conf/cacerts -storepass changeit
```

Example:

```
keytool -importcert -file /home/admin/ldap-server.crt -alias
ldap-server -keystore /etc/alternatives/jre_17/lib/security/cacerts
-storepass changeit
```

Following is the location for Keycloak certificate: /etc/alternatives/jre_17/lib/security/

Next steps

Configuring LDAPS in Keycloak

Configuring LDAPS in Keycloak

Procedure

1. Login to Keycloak Admin Console.
2. In the left navigation pane, go to the realm where you want to configure LDAP.
3. If you are using the default realm, select **Master** or the custom realm you want to configure.
4. Click **User Federation** under **Realm Settings**.
5. Click **LDAP** to configure LDAP.
6. Click **Add provider** and select **ldap**.

 Note:

For LDAPS, ensure the connection URL starts with *ldaps://*.

7. Enter the required LDAP connection details.
8. In the **Use Truststore SPI** field, select **IdapsOnly** if you have configured a custom truststore.
9. Disable the **Enable StartTLS** option.
10. Click **Test authentication** to connect Keycloak to your LDAP server.
11. Save the configuration.

Example

Following are the configuration examples:

```
plaintext
Copy code
Vendor: Other
Connection URL: ldaps://ldap.example.com:636
Bind Type: simple
Bind DN: cn=admin,dc=example,dc=com
Bind Credential: <your password>
```

Configuring the LDAP UID mapping

About this task

When configuring SSO, ensure that the value of the UID mapping attribute is set for each LDAP server according to the value of **Access token email address attribute**, which is provided in the identity provider mapping.

In **Access token email address attribute**, you can see one of the following options:

- email
- samAccountName

- `userPrincipalName`

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal with the Security administrator role.
2. Navigate to **Security Settings > Client ID Mapping**.
3. Click **Edit**.
Avaya Aura® Device Services displays the identity provider mapping settings.
4. Note the **Access token email address attribute** value.
5. Click **Cancel**.
6. Navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
7. Click the appropriate LDAP server.
8. If **Access token email address attribute** is set to `email`, in the Modify LDAP Attribute Mappings section, record the **EmailAddress** value.
9. In the Server Address and Credentials section, in **UID Attribute ID**, do one of the following:
 - For `email` in **Access token email address attribute**, enter the value you recorded in **EmailAddress**.
 - For `samAccountName` in **Access token email address attribute**, enter `samAccountName`.
 - For `userPrincipalName` in **Access token email address attribute**, enter `userPrincipalName`.
10. If additional LDAP servers are configured on Avaya Aura® Device Services, repeat steps 7 to 9 for each LDAP server.

Synchronizing data between Avaya Aura® Device Services and an identity provider

About this task

Avaya Aura® Device Services periodically synchronizes data, such as public keys, with identity providers. To ensure that Avaya Aura® Device Services and the identity provider contains the up-to-date data, you can synchronize data manually.

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal with the Security administrator role.

2. Navigate to **Security Settings > Client ID Mapping**.
3. Click **Sync** for the required client.
4. After the synchronization completes, click **OK** in the confirmation window.

Testing the integration with an identity provider from the Google Chrome web browser

About this task

Use this procedure to verify that the integration with an identity provider using OAuth2 is configured correctly. Use the Google Chrome web browser for this procedure.

Important:

For testing purposes, you will disable the web security of the Chrome browser when performing the procedure. After performing this procedure, you *must* close this browser instance and then restart the browser.

Before you begin

You must have an Avaya Workplace Client user account.

Procedure

1. Do the following to run the Google Chrome web browser with web security disabled:
 - a. Use the CLI to navigate to the Chrome web browser executable file location.
For example: `cd "\Program Files (x86)\Google\Chrome\Application"`
 - b. Run the following command:

```
chrome --disable-web-security --user-data-dir=%TMP%
```

2. In the browser address bar, enter the following URL:

```
https://<AADS_FQDN>:<AADS_PORT>/acs/resources/authorize?
client_id=Equinox&app_cb_uri=https://<AADS_FQDN>:<AADS_PORT>/
```

In this address, <AADS_FQDN> is the Avaya Aura® Device Services front-end FQDN and <AADS_PORT> is the Avaya Aura® Device Services front-end service port.

Note:

In a cluster environment, if you use front-end port 443, you must use the Avaya Aura® Device Services front-end FQDN or virtual IP address.

3. If more than one identity provider is configured on Keycloak, on the Login page, click the identity provider you want to test.

For example, if you want to test the integration with Office 365, click **Microsoft**.

4. If you are logging in for the first time, on the Permissions page, click **Accept**.
5. Enter your Avaya Workplace Client credentials.

If the authentication process completes successfully, Chrome displays a JSON response containing information about an access token and a refresh token. The following is an example of the response:

```
{
  "access_token": "<access token value>",
  "expires_in": 1800,
  "refresh_expires_in": 3600,
  "refresh_token": "<refresh token value>",
  "token_type": "bearer",
  "not-before-policy": 0,
  "session_state": "<session state value>",
  "scope": "profile pmm aads email"
}
```

6. Close the web browser instance.

Testing the integration with the identity provider from the web administration portal

About this task

Use this procedure to verify that the integration with the identity provider is configured successfully and clients can use SSO capabilities.

Before you begin

- Configure the identity provider.
- Configure the Keycloak settings as described in [Configuring Keycloak settings](#) on page 124.
- Configure the attribute mapping as described in [Modifying the attribute mapping between the third-party identity provider and Keycloak](#) on page 133.
- Configure client mapping as described in [Creating client mapping](#) on page 126.
- Obtain an Avaya Workplace Client user account that you use to test authorization.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Security Settings > Client ID Mapping**.
2. Click **Test** for the required client.
Avaya Aura® Device Services displays the Test Integration window.
3. In the Test Integration window, click the **Start Test** button.
Your browser opens the Login page in a new tab.
4. If you have multiple identity providers configured, select the identity provider that you want to test.

Your browser opens the Login page for the selected identity provider.

5. Enter the username and password of the test user and then click the **Sign On** button.

The exact button name might differ from the name listed above depending on the identity provider that you are testing.

If the test completes successfully, the browser displays the `Token generated, You may close this window` message. The Avaya Aura® Device Services web administration portal displays the `Test completed successfully` message, the test user information, and token details in the Test Integration window.

If the test fails, Avaya Aura® Device Services displays information about the error in the Test Integration window.

6. Do one of the following:
 - If the verification completes successfully, click **OK**.
 - If the verification fails, try to fix the issue by checking the prerequisites for the test, and then re-run the test.
 - If the problem persists, contact Avaya support personnel.

OAuth2 testing status

The following table shows status messages that Avaya Aura® Device Services can display depending on the OAuth2 test results.

Status	Test result	Description/Solution
Test Id generated	In Progress	Test is in progress.
SAML token from IDP received	In Progress	Avaya Aura® Device Services received a token from the identity provider.
Access token generated successfully	In Progress	The identity provider generated an access token successfully.
Generated token is valid	Successful	Avaya Aura® Device Services validated the token. Test completed successfully.
Generated token is invalid	Failed	The identity provider generated a token, but one or more mandatory parameters are missing in the token.
Scope is empty, Scope validation failed.	Failed	Client scopes are not configured on Keycloak. Ensure that Keycloak is correctly configured. For more information, see Configuring Keycloak settings on page 124 and Modifying the attribute mapping between the third-party identity provider and Keycloak on page 133.
JWT Signature validation failed	Failed	The generated token might be tampered. Re-run the test.

Status	Test result	Description/Solution
JWT Token is expired.	Failed	Increase the access token lifespan. For more information, see Configuring access and refresh token expiry times on page 149.
No supported roles/No username provided in token.	Failed	• Ensure that the user has the valid email ID. • Ensure that the role mapping is configured, and the user has application roles. For more information, see Modifying the attribute mapping between the third-party identity provider and Keycloak on page 133.
Exception in generating token from IDP code	Failed	The identity provider sent the code, but Avaya Aura® Device Services could not generate a valid token. Avaya Aura® Device Services displays this general error message when the exact error category cannot be determined.
Keycloak is unavailable.	Failed	The Keycloak service is unavailable. Restart Keycloak. For more information, see Starting and stopping the Keycloak service on page 126.

Configuring access and refresh token expiry times

About this task

The access token lifetime determines the time period during which Avaya Workplace Client does not prompt the user to re-authenticate. Refresh tokens are used to refresh the access token lifetime. You can use the Keycloak service to configure the lifetime for access and refresh tokens. The main settings are the following:

- **Access Token Lifespan:** Sets the expiry time for access tokens.
- **SSO Session Idle:** Sets the expiry time for refresh tokens. If the refresh token is not used by the expiry time, then the Avaya Workplace Client user needs to log in again to get new access and refresh tokens.
- **SSO Session Max:** Sets the overall maximum time period for refresh tokens. During this time, refresh tokens can be used to obtain new access tokens.

The choice of a lifespan for tokens is a trade-off between security and user experience impact:

- If the token lifespan is too long, it increases the opportunity for a malicious actor to capture the tokens.
- If the token lifespan is too short, Avaya Workplace Client frequently prompts users to log in again.

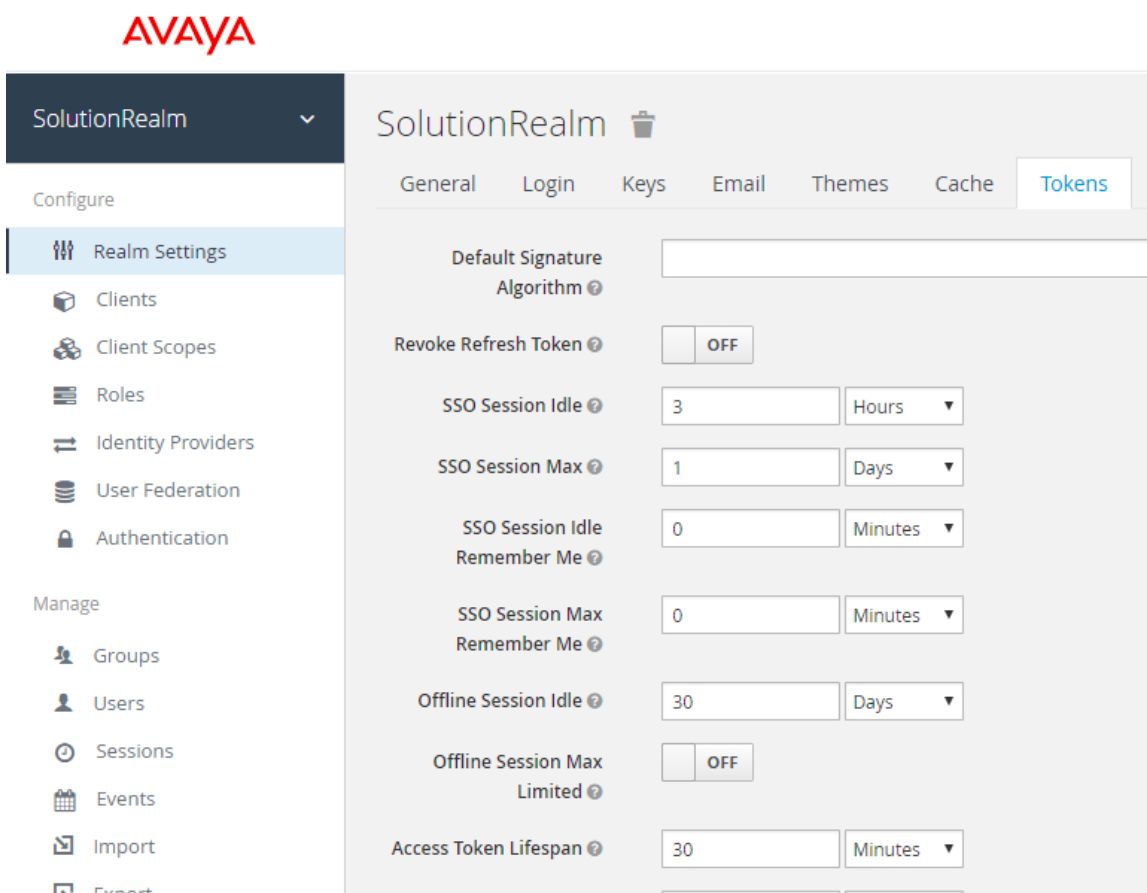
For more information and recommendations, see [Access and refresh token expiry times](#) on page 49.

Procedure

1. On the Keycloak web administration portal, navigate to **SolutionRealm** and then click **Realm Settings**.
2. In the right area, click **Tokens**.
3. Configure the expiry time for the following settings:
 - **SSO Session Idle**
 - **SSO Session Max**
 - **Access Token Lifespan**
4. Click **Save**.

Example

The following is an example of expiry times configuration:



The screenshot shows the Avaya Aura® Device Services Single Sign-On management interface. The top navigation bar includes the Avaya logo and a dropdown menu for 'SolutionRealm'. The left sidebar contains a 'Configure' section with 'Realm Settings' selected, and a 'Manage' section with options like Groups, Users, Sessions, Events, Import, and Export. The main content area is titled 'SolutionRealm' and has tabs for General, Login, Keys, Email, Themes, Cache, and Tokens. The 'Tokens' tab is active, displaying various configuration settings for tokens. The settings include Default Signature Algorithm, Revoke Refresh Token (set to OFF), SSO Session Idle (3 Hours), SSO Session Max (1 Days), SSO Session Idle Remember Me (0 Minutes), SSO Session Max Remember Me (0 Minutes), Offline Session Idle (30 Days), Offline Session Max Limited (set to OFF), and Access Token Lifespan (30 Minutes).

Related links

[Access and refresh token expiry times](#) on page 49

Blocking access to the Avaya Authorization service

About this task

Use this procedure if you need to prevent a previously logged in user from logging in to Avaya Aura® Device Services using the third-party identity provider.

Procedure

1. On the Keycloak web administration interface, navigate to your realm and then click **Users**.
2. In the **Search** field, enter the user name and then click .
Avaya Aura® Device Services displays the list of users.
3. Click the **Edit** button located to the right of the required user name.
Avaya Aura® Device Services displays the user profile page.
4. On the Details tab, set **User Enabled** to **OFF**.
5. Click **Save**.

Enabling OAuth database replication in a cluster environment

About this task

In a cluster environment, you must have a copy of the OAuth database on each cluster node. Use this procedure to enable OAuth database replication. If your deployment includes OAuth, you must perform this procedure in the following cases:

- After installing Avaya Aura® Device Services
- After performing a migration
- After rolling back Avaya Aura® Device Services
- Before restoring Avaya Aura® Device Services

Note:

You do not need to perform this procedure after upgrading Avaya Aura® Device Services. After upgrading, Avaya Aura® Device Services enables OAuth database replication automatically.

Procedure

Perform steps 1 to 6 on the seed node first and then on all non-seed nodes.

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the configuration utility using the `app configure` command.
3. Select **Enable OAuth Cluster**.

4. Select **Enable OAuth Cluster** again and then enter `y`.
5. Select **Exit**.
6. Select **Yes** and then select **Apply**.
7. On the seed node, run the `svc aads restart` command to restart Avaya Aura® Device Services and then wait until the restart process is completed.
8. On all non-seed nodes, run the `svc aads restart` command to restart Avaya Aura® Device Services.

Keycloak log management

Avaya Aura® Device Services collects Keycloak logs along with other system logs.

You can collect Keycloak logs from the Log Management section of the Avaya Aura® Device Services web administration portal. For more information, see [Downloading logs](#) on page 336.

 Note:

For the keycloak service, only the **WARN** log, also known as the default log level, is currently available. You cannot change the keycloak log level.

Chapter 5: Avaya Spaces integration

Avaya Spaces is a cloud-based team collaboration and meeting platform. Avaya Spaces integrates multiple forms of communication, such as voice, video, instant messaging, and screen-sharing, into a single application that can be used on different platforms.

Using the Avaya Aura® Device Services web administration portal, you can:

- Create and register users in your enterprise on Avaya Spaces. These users do not need to perform the user self-registration sign-up process.
- Allocate licenses to users without having to wait until they log in to Avaya Spaces. You can use the Avaya Aura® Device Services web administration portal as a single administration point for managing Avaya Spaces licenses.

 Note:

From the Avaya Aura® Device Services web administration portal, you can allocate licenses only to enterprise users registered on Avaya Spaces. To manage licenses for users created on Avaya Spaces, use the Avaya Spaces administration portal.

Checklist for configuring Avaya Spaces integration

Use this checklist to configure integration with Avaya Spaces.

No.	Task	Notes	✓
1	Set up an Avaya Spaces account.	See Avaya Spaces account configuration on page 154. Skip this step if you already have an Avaya Spaces account and you configured your company on Avaya Spaces. Avaya also recommends that you enable Enterprise SSO on Avaya Spaces.	
2	Obtain an Avaya Aura® Device Services API key and API key secret for your company on Avaya Spaces.	See Obtaining an API key and API key secret on page 156.	

No.	Task	Notes	✓
3	Configure Avaya Spaces settings on Avaya Aura® Device Services.	See Setting up Avaya Spaces integration on page 156.	
4	Optionally, configure the LDAP user deletion warning.	See sections under LDAP user deletion confirmation on page 204.	
5	Manage Avaya Spaces users and licenses.	See User and license management overview on page 163.	

Avaya Spaces account configuration

To manage Avaya Spaces users on Avaya Aura® Device Services, you must create and configure an Avaya Spaces account. This account stores the parameters required to authorize your Avaya Aura® Device Services system on Avaya Spaces.

Use the following sections to create and configure your Avaya Spaces account.

Setting up a company and domain in Avaya Spaces

About this task

You must provide the company domain associated with your Avaya Aura® Device Services system.

For more information, see the [Configuring a company](#) in *Avaya Spaces User Manual*.

Procedure

1. Log in to <https://accounts.avayacloud.com/> as an administrator.
2. If you have not set up your company or want to configure a new company, do the following:
 - a. Click on your user name in the top-right area of the screen and then click **Add Company**.
 - b. Type a name and description for your company.
 - c. Click **Save**.
3. Click **Manage Companies** and click the existing company name.
4. Click the **Domains** tab.
5. Click **Add Domain**.
6. Enter the domain name and then click **OK**.
7. To verify ownership of the domain, next to the domain name, click **Verify**.
8. Do one of the following:
 - Follow the on-screen instructions to add the verification code to your domain account and then click **Verify**.

- At the bottom-right area of the Verify Domain window, click **Manual Verify** to have Avaya personnel verify the ownership of the domain.

Related links

[Obtaining an API key and API key secret](#) on page 156

[Disabling Avaya Spaces integration](#) on page 180

Creating an API key

About this task

To access Avaya Spaces services, you must create an API key for your company and then provide this key and associated API key secret on Avaya Aura® Device Services. An API key secret is created automatically when you create an API key.

Procedure

1. Log in to Avaya Spaces at <https://accounts.avayacloud.com/> as an administrator.
2. In the left pane, click **Manage Companies**.
3. Select your company from the list.
4. Click the **API Key** tab.
5. Click **Add API key +**.
6. In the Add API key window, select **AADS** from the drop-down list and then click **Add API key**.

You can also type **AADS** in the search field. Avaya Spaces only displays entries that contain the text you entered.

Avaya Spaces displays the new key in the API Keys table.

The use of Enterprise SSO for Avaya Spaces integration

Avaya recommends that you enable Enterprise SSO on Avaya Spaces before configuring integration between Avaya Aura® Device Services and Avaya Spaces. When Avaya Aura® Device Services creates a user on Avaya Spaces, Avaya Spaces assigns a random password to this user, but Avaya Aura® Device Services does not have information about this password. Therefore, when a user tries to log in to Avaya Spaces, one of the following occurs depending on whether Enterprise SSO is enabled:

- If Enterprise SSO is enabled, the user should log in to Avaya Spaces using the Enterprise SSO login option. The user enters their enterprise credentials to log in.

If these users need to change their passwords, they must contact their enterprise IT service.

- If Enterprise SSO is disabled, the user must use the “Forgot Password” functionality to set up their password first. After the password is set up, the user can log in to Avaya Spaces.

Obtaining an API key and API key secret

About this task

Each company that is registered on Avaya Spaces has an associated API key and key secret. Avaya Aura® Device Services requires these values to access Avaya Spaces services.

Before you begin

- Ensure that your company and domain are configured in Avaya Spaces.
- Ensure that at least one API key with the “AADS” role is configured for your company in Avaya Spaces.

Procedure

1. Log in to Avaya Spaces at <https://accounts.avayacloud.com/> as an administrator.
2. In the left pane, click **Manage Companies**.
3. Select your company from the list.
4. Click the **API Key** tab.
5. From the API Keys table, copy the API key with the “AADS” role that you want to use and save it on your computer.
6. In the API Keys table, click **View/Edit** for the API key you copied.
7. In the Secret area, click  to copy the API key secret to the clipboard and save it on your computer.

Setting up Avaya Spaces integration

About this task

You can set up integration with a specific company configured on your Avaya Spaces account. When integration is set up, you can use the Avaya Aura® Device Services web administration portal to view and manage users for that company.

You can have multiple companies configured on your Avaya Spaces account. However, Avaya Aura® Device Services only supports integration with one company at a time. If you want to set up integration for another company, you must delete the existing configuration first.

Note:

As of Release 8.0.2, Avaya Aura® Device Services contains all required Avaya Spaces CA certificates in a separate public CA truststore, so you do not need to import these certificates manually.

Before you begin

- Configure Enterprise SSO on Avaya Spaces.

If Enterprise SSO is enabled, new Avaya Spaces users created on Avaya Aura® Device Services do not need to reset their passwords before logging in to Avaya Spaces for the first time.

- Obtain the API key and API key secret for the Avaya Spaces company that you are planning to use for integration.
- Ensure that you have at least one verified domain for the company.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces > Configuration**.
2. Select the **Enable Spaces Integration** check box.
3. In **Spaces URI**, enter `accounts.avayacloud.com`.

If required, you can provide a new value later without having to set up integration again.

4. In **Spaces API Key**, enter the API key that you copied from Avaya Spaces.
5. In **Spaces API Key secret**, enter the API key secret that you copied from Avaya Spaces.
6. In **LDAP Phone Number Sync**, select which user phone numbers configured on LDAP you want to synchronize with Avaya Spaces accounts:

- **All (Work and Mobile)**: To synchronize work and mobile phone numbers.
- **Work**: To synchronize only the work phone number configured in LDAP.
- **Mobile**: To synchronize only the mobile phone number configured in LDAP.
- **None**: To not synchronize work or mobile phone numbers.

The numbers you selected for synchronization are added to the list of numbers configured on Avaya Spaces, and do not affect already existing Avaya Spaces phone numbers.

7. Click **Save**.

Result

When the integration process is completed, Avaya Aura® Device Services notifies you and automatically populates the following fields:

- **Company Name**: Shows the name of the Avaya Spaces company for which you are setting up integration.
- **Domain**: Shows all verified domain names configured for the company in Avaya Spaces.
- **Status**: Shows the connection status.
- **License Information**: Shows information about the available advanced licenses and license expiration dates.

Next steps

- Configure data synchronization between Avaya Aura® Device Services and Avaya Spaces.
- Update language and time zone databases.

Related links

[Setting up a company and domain in Avaya Spaces](#) on page 154

[Obtaining an API key and API key secret](#) on page 156

[Disabling Avaya Spaces integration](#) on page 180

[Updating Avaya Spaces integration parameters](#) on page 179

[Avaya Spaces integration settings](#) on page 179

[Avaya Aura Device Services does not contain the latest Avaya Spaces CA certificate](#) on page 423

Configuring data synchronization between Avaya Aura[®] Device Services and Avaya Spaces

About this task

Use this procedure to synchronize user data, licensing, and company domain information between Avaya Aura[®] Device Services and Avaya Spaces. You can configure automatic synchronization on a scheduled date or at a specific time interval. You can also synchronize user data manually.

When synchronization is enabled, Avaya Aura[®] Device Services synchronizes user data in the following cases:

- When you synchronize data manually.
- During scheduled synchronization events.

When Avaya Aura[®] Device Services synchronizes data with Avaya Spaces, the user management functionality on the Assign License and View and Manage pages is unavailable.

If Avaya Aura[®] Device Services cannot synchronize data, it displays an error message on the Configuration page. If synchronization fails because of a connection issue, Avaya Aura[®] Device Services also raises an alarm.

If synchronization is disabled, Avaya Aura[®] Device Services only stores Avaya Spaces configuration data.

Before you begin

Enable Avaya Spaces integration.

Procedure

1. On the Avaya Aura[®] Device Services web administration portal, navigate to **Spaces > Configuration**.
2. Select the **Enable user license synchronization** check box.
3. In the Spaces Configuration area, click **Save**.
4. In the User Synchronization Update Instructions area, specify the date and time when you want to synchronize user data.
5. To configure scheduled synchronization, select the **Repeat every** check box and then specify the period between consecutive synchronization attempts.

Scheduled synchronization starts from the time and date that you specified in the previous step.

6. **(Optional)** To immediately synchronize user data, click **Force Sync**.

Immediate synchronization does not affect scheduled synchronization.

7. Click **Save**.

Example

The following example shows an automatic synchronization update that starts on May 4, 2022 at 5:00 p.m. and then repeats daily:

User Synchronization Update Instructions

Last Sync Status : as on :

2022-05-04 5:00 ▼ PM ▼ (UTC+5:30)

☒ Repeat every 1 ▼ day ▼

Force Sync Save Cancel Stop

Related links

[Setting up user synchronization with the LDAP server](#) on page 202

[Viewing the Avaya Spaces connection status](#) on page 181

[Avaya Aura Device Services alarms list](#) on page 342

[Avaya Spaces connectivity errors](#) on page 422

[Avaya Spaces pages blocked](#) on page 425

Stopping synchronization with Avaya Spaces

About this task

You can stop a running data synchronization gracefully if the synchronization is stuck in the "In Progress" state.

Stopping a running synchronization does not affect scheduled synchronization.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces > Configuration**.
2. In the User Synchronization Update Instructions area, click **Stop**.
The synchronization status changes to "Stopped".

Phone number synchronization

For enterprise users registered on Avaya Spaces, you can enable synchronization for work and mobile phone number types. When you enable synchronization for a specific phone number type, Avaya Aura® Device Services imports appropriate phone numbers configured on LDAP into Avaya Spaces user profiles. Therefore, when phone number synchronization is enabled, Avaya Spaces user profiles contain both phone numbers configured on Avaya Spaces and phone numbers imported from LDAP.

Avaya Aura® Device Services updates the imported numbers in the Avaya Spaces database when synchronizing data with Avaya Spaces or LDAP.

Avaya Spaces and LDAP numbers are controlled by Avaya Spaces and LDAP respectively. You cannot modify LDAP numbers from the Avaya Spaces administration portal. If you try to modify an imported number, Avaya Aura® Device Services will revert changes when synchronizing data between Avaya Aura® Device Services and Avaya Spaces databases. From the Avaya Spaces administration portal, you can modify Avaya Spaces numbers and cannot modify LDAP numbers.

Note:

If the same phone number is configured for a user both on Avaya Spaces and in LDAP, Avaya Aura® Device Services considers this phone number as an LDAP phone number.

When you disable synchronization for a specific phone number type, Avaya Aura® Device Services removes from user profiles all phone numbers of that type that were imported from LDAP. Phone numbers of that type configured on Avaya Spaces remain in user profiles.

Important:

If the same phone number is configured for a user both on Avaya Spaces and in LDAP, then, when you disable phone number synchronization, Avaya Aura® Device Services removes this phone number from the user's Avaya Spaces profile.

Configuring phone number synchronization

About this task

For enterprise users registered on Avaya Spaces, you can synchronize mobile and work phone numbers between Avaya Spaces and LDAP databases. When synchronization is enabled for a certain phone number type, Avaya Aura® Device Services exports appropriate phone numbers from LDAP to Avaya Spaces. As a result, Avaya Spaces user profiles contain both phone numbers configured on Avaya Spaces and phone numbers imported from LDAP.

Before you begin

Enable integration with Avaya Spaces.

Procedure

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

2. In the LDAP Phone Number Sync section, select one of the following:
 - **All (Work and Mobile):** To add both work and mobile phone numbers from LDAP to Avaya Spaces.
 - **Work:** To add to Avaya Spaces work phone numbers from LDAP. Mobile phone numbers imported from LDAP will be removed from Avaya Spaces.
 - **Mobile:** To add mobile phone numbers from LDAP to Avaya Spaces. Work phone numbers imported from LDAP will be removed from Avaya Spaces.
 - **None:** To remove and work phone numbers imported from LDAP from Avaya Spaces.
3. Click **Save**.
 Avaya Aura® Device Services will update LDAP phone numbers in the Avaya Spaces database according to the new synchronization settings after manual or automatic synchronization between Avaya Aura® Device Services and Avaya Spaces.
4. **(Optional)** In the User Synchronization Update Instructions area, click **Force Sync** to synchronize phone numbers immediately.

Uploading Avaya Spaces language and time zone settings to Avaya Aura® Device Services

About this task

Avaya Aura® Device Services does not automatically receive information about languages and time zones in Avaya Spaces. You must manually upload new language and time zone settings, which are available on Avaya Spaces, using the `clitool` command.

Before you begin

- Obtain the list of Avaya Spaces languages and time zone settings from the Avaya Spaces administrator.
- Prepare text files containing information about Avaya Spaces languages and time zones. For more information about file formats, see [Language file format](#) on page 162 and [Time zone file format](#) on page 163.

Procedure

1. Use a file transfer utility, such as SFTP or SCP, to upload files with information about languages and time zones to a directory with read rights for `clitool`.

For example, upload the files to `/opt/Avaya/DeviceServices/<version number>/`

2. Run the `cdto misc` command.
3. To update languages do one of the following:
 - To replace the existing languages with the languages from the file, run the following command:

```
sudo ./clitool-acs.sh languageORTimeZoneUpdate
<PATH_TO_LANGUAGES> true true
```

- To add the languages from the file in addition to the existing languages, run the following command:

```
sudo ./clitool-acs.sh languageORTimeZoneUpdate
<PATH_TO_LANGUAGES> true false
```

In these commands, `<PATH_TO_LANGUAGES>` is the full path to the file containing new languages. For example, `/opt/Avaya/DeviceServices/10.1.0.0.88/language.properties`

4. To update time zones, do one of the following:

- To replace the existing time zones with the time zones from the file, run the following command

```
sudo ./clitool-acs.sh languageORTimeZoneUpdate
<PATH_TO_TIMEZONES> false true
```

- To add the time zones from the file in addition to the existing time zones, run the following command:

```
sudo ./clitool-acs.sh languageORTimeZoneUpdate
<PATH_TO_TIMEZONES> false false
```

In these commands, `<PATH_TO_TIMEZONES>` is the full path to the file containing new time zones. For example, `/opt/Avaya/DeviceServices/10.1.0.0.88/timezone.properties`

Language file format

The UTF-8 text file containing new languages for Avaya Spaces can have any name and extension. For example, `language.properties`. The file contains a sequence of `language=code` pairs, where:

- `language` is the name of the language, which is displayed on the Avaya Aura® Device Services web administration portal. For example: `français (Canada) - French (Canada)`
- `code` is the language and locale code. For example, `fr-CA`. This code uses the `LL[-CC]` format where:
 - `LL` is a language code. The language code is represented by two lowercase letters. For example: `fr`. For more information about codes, see [ISO 639-1](#).
 - `CC` is an optional country code. The country code is represented by two uppercase letters. For example: `CA`. For more information about codes, see [ISO 3166-1](#).

Each pair must be on a separate line.

The following is an example of a language file:

```
English=en-US
Deutsch - German=de-DE
español - Spanish=es-LA
```

```
français (Canada) - French (Canada)=fr-CA
français (France) - French (France)=fr-FR
italiano - Italian=it-IT
日本語 - Japanese=ja
한국어 - Korean=ko-KR
```

Time zone file format

The text file containing new Avaya Spaces time zones can have any name and extension. For example, `timezone.properties`. The file contains a sequence of time zones in the `area/location Olson name` format. For example, `America/New_York` or `Europe/Isle_of_Man`. Each time zone must be on a separate line.

The following is an example of a time zone file:

```
Africa/Addis_Ababa
Atlantic/Stanley
Atlantic/Faroe
Pacific/Fiji
Europe/Helsinki
Europe/Paris
America/Cayenne
Pacific/Gambier
```

User and license management overview

After setting up Avaya Spaces integration, you can:

- Register users in your enterprise on Avaya Spaces.
- View Avaya Spaces users.

Avaya Aura® Device Services displays both users created on Avaya Spaces and users in your enterprise that you registered on Avaya Spaces.

- Allocate Avaya Spaces licenses to users in your enterprise registered on Avaya Spaces.

Note:

You cannot use the Avaya Aura® Device Services web administration portal to manage licenses for users created on Avaya Spaces. To manage licenses for these users, use the Avaya Spaces administration portal.

Enterprise user registration on Avaya Spaces

You can register users that are configured in your enterprise LDAP directory on Avaya Spaces. The registration process includes the following steps:

1. Selecting users in your enterprise that you want to register on Avaya Spaces.

You can only register users with an assigned email address.

2. Registering the selected users on Avaya Spaces.

Avaya Aura® Device Services displays the users selected for registration on the Assign License page. The selected users can have the following status:

Status	Status name	Description
To be processed	TO_BE_PROCESSED	The user is ready for registration on Avaya Spaces.
In progress	IN_PROGRESS	User registration is in progress.
Cancelled	CANCELLED	The user registration operation is canceled.
Failed	FAILED	The user registration failed.

Avaya Aura® Device Services displays the registered users on the View and Manage page.

Avaya Spaces user licenses

All Avaya Spaces users have the Essential license by default. If a user requires additional features, you can assign a Business or Power license to them. The number of available licenses is dependent on how many Business and Power licenses your company purchased. For more information about Avaya Spaces user licenses, see “Assigning Users” and “Plans” in *Using Avaya Spaces*.

When configuring an enterprise user for registration on Avaya Spaces, you can select a license option. After registering the user on Avaya Spaces, you can allocate a different license type for that user if required.

All licenses of the same license type have the same expiration date.

Trial licenses

Avaya Spaces offers trial Business and Power licenses. Trial licenses provide access to the same features as the advanced licenses but for a limited amount of time.

Avaya Spaces assigns trial licenses automatically. If you select the Essential license when configuring an enterprise user for registration on Avaya Spaces, then, when the user logs in to Avaya Spaces for the first time, the Essential license is converted to the Business Trial license or the Power Trial license. The default trial license is the Business Trial license, even if the company does not have any purchased licenses. You *cannot* assign trial licenses manually when configuring enterprise users for registration on Avaya Spaces. Trial licenses are personal.

If you have available Business or Power licenses, you can update the user’s trial license to either Business or Power license at any time. After the trial period expires, Avaya Spaces keeps the trial license for a user until the user logs in to Avaya Spaces. When the user logs in, Avaya Spaces assigns the Essential license to this user.

Trial licenses are per-user licenses, therefore each trial license has its own expiration date.

Avaya Aura® Device Services displays trial licenses as “Business (Trial)” and “Power (Trial)”.

Avaya Spaces licensing information on Avaya Aura® Device Services

When data synchronization is enabled, Avaya Aura® Device Services retrieves information about licenses from Avaya Spaces, including the following:

- The number of available licenses.
- The license expiration date for Business, Power, and Trial licenses.

Avaya Aura® Device Services displays this information on the Configuration page. Avaya Aura® Device Services also displays information about license expiration dates on the View and Manage page.

If a license expired or will expire soon, Avaya Aura® Device Services displays a warning message when you:

- Add enterprise users for registration on Avaya Spaces.
- Review Avaya Spaces users on the Configuration page.
- Assign a different license to a Avaya Spaces user.

Adding enterprise users for registration on Avaya Spaces

About this task

Use this procedure to:

- Select users from your enterprise LDAP directory that you want to register on Avaya Spaces.
- Provide configuration details for these users, such as the appropriate Avaya Spaces license type, time zone, and language.

You can select a single user or an LDAP group. When you select an LDAP group, you can add all users from that group or select specific users of that group. You cannot select an LDAP group that is configured for automatic registration of group members on Avaya Spaces. You also cannot select a user that belongs to an LDAP group that is configured for automatic registration.

After adding a user using this procedure, you can only modify the selected license type. Therefore, if you need to change other data, such as the time zone or language, you must remove and then re-add the user.

You must ensure that the domain part of the user's email address matches one of your company domains configured on Avaya Spaces. Otherwise, the registration procedure will fail.

You can only add enterprise users with an assigned email address.

Before you begin

If you are planning to assign advanced Avaya Spaces user licenses, ensure that you have enough licenses of the required type.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces > Users and License > Assign License**.
2. From the drop-down list, select one of the following:
 - **User:** To select a single enterprise user.
 - **Group:** To select users from an LDAP group.
3. In **Search User/Group**, enter the following search criteria:
 - To find a user, type their name or email address.
 - To find an LDAP group, type the group name.

Avaya Aura® Device Services displays the entries that contain the text you entered. If a user does not have an email address, the entry contains `(null)` after the user name. For example: John Doe `(null)`.

4. **(Optional)** If you select an LDAP group, you can do the following to select specific users of that group for registration:
 - a. Click **Filter**.

Avaya Aura® Device Services displays the list of users belonging to the selected LDAP group. By default, all users of this group are selected for registration on Avaya Spaces.
 - b. Clear check boxes for users that you do not want to register on Avaya Spaces.
 - c. Click **Submit**.
5. From **License**, select an Avaya Spaces license to assign to the user.

You can update the license type later when you are registering the user on Avaya Spaces.
6. **(Optional)** From **Time Zone**, select a time zone for the user.

The list contains time zones available on Avaya Spaces. If you leave this field blank, the default time zone for your Avaya Spaces company is used.
7. **(Optional)** From **Language**, select a language for the user.

The list contains languages available on Avaya Spaces. The default language is English.
8. Click **Add**.

If the enterprise user does not have an email address, Avaya Aura® Device Services displays an error message. Otherwise, Avaya Aura® Device Services adds the selected user to the table on the Assign License page.

Next steps

Register the selected enterprise users on Avaya Spaces.

Related links

[Registering enterprise users on Avaya Spaces](#) on page 166

[Removing an unregistered user](#) on page 167

[Avaya Spaces user licenses](#) on page 164

Registering enterprise users on Avaya Spaces

About this task

After adding enterprise users, you can start the registration process. When registration is complete, enterprise users can use Avaya Spaces services.

You can also use this procedure to re-register users with the “CANCELLED” or “FAILED” status.

After starting the registration process, you cannot start the new registration process until:

- Avaya Aura® Device Services processes all users.
- You cancel the registration process.

The registration functionality is unavailable when Avaya Aura® Device Services:

- Synchronizes data with an LDAP server.

- Synchronizes data with Avaya Spaces.
- Performs the Avaya Spaces user audit.

Before you begin

Add enterprise users as described in [Adding enterprise users for registration on Avaya Spaces](#) on page 165.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces > Users and License > Assign License**.

Avaya Aura® Device Services displays the users you added for registration.

2. **(Optional)** To select another Avaya Spaces license for a user, click the **Assigned License** field for the user and then select the required license from the drop-down list.

You cannot select another license for a user in the following cases:

- The user belongs to an LDAP group configured for automatic registration.
- Registration is in progress for the user.

3. Click **Assign**.

Result

Avaya Aura® Device Services starts the registration process for all users and changes their status to "TO_BE_PROCESSED". When Avaya Aura® Device Services starts processing a user, the user status changes to "IN_PROGRESS". When the user is registered on Avaya Spaces, Avaya Aura® Device Services no longer displays the user on the Assign License page. Instead, the user is displayed on the View and Manage page.

Avaya Aura® Device Services displays the results of the registration process on the Assign License page.

Related links

[Cannot register an enterprise user on Avaya Spaces](#) on page 424

[Cancelling user registration and license upgrade operations](#) on page 178

Removing an unregistered user

About this task

Use this procedure to remove a user from the list of users you selected for registration on Avaya Spaces. For example, you must remove a selected for registration user and then re-add that user if you want to modify user's time zone or language.

Note:

You can modify a license type for a user selected for registration.

You cannot remove with the "TO_BE_PROCESSED" or "IN_PROGRESS" status.

When you use this procedure to remove a user, that user is *not* removed from your enterprise LDAP directory.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces > Users and License > Assign License**.
2. Do one of the following:
 - To select a single user, select the check box next to the user's name or search for the user by typing a user name or email address in the **Search** field.
 - To select multiple users, select the check boxes for the required users.
 - To select all users in bulk, select the **Select all** check box.
3. Click **Delete**.

Avaya Aura® Device Services removes all selected users from the list of users selected for registration.

Related links

[Cannot register an enterprise user on Avaya Spaces](#) on page 424

Automatic registration of LDAP group members on Avaya Spaces

Avaya Aura® Device Services enables you to automatically register enterprise users that belong to a specific LDAP group. When a new user is added to a group that uses automatic registration functionality, Avaya Aura® Device Services registers that user on Avaya Spaces. If a user is removed from that group, Avaya Aura® Device Services automatically removes that user from Avaya Spaces.

Important:

Avaya Aura® Device Services receives information about the status and members of LDAP groups when synchronizing data with the enterprise LDAP server. Therefore, you must enable periodic synchronization with your LDAP server to use the automatic registration functionality. You can use manual synchronization if you need to register new LDAP group users on Avaya Spaces immediately.

User settings provided through automatic registration take priority over manual registration settings provided on the Assign License page.

When an LDAP group is configured for automatic registration, you can only manage settings for the entire group. For example, you cannot update a user's license or remove a user from Avaya Spaces if the user is a member of an LDAP group that uses automatic registration. If you try to remove an automatically registered user from Avaya Spaces, Avaya Aura® Device Services will re-register this user on Avaya Spaces during the next synchronization with Avaya Spaces.

For users that are automatically registered on Avaya Spaces, Avaya Aura® Device Services displays the LDAP group's Distinguished Name (Group DN) on the View and Manage page in the **Registered GroupDN** field.

If you delete or rename an LDAP group that is configured for automatic registration, Avaya Aura® Device Services removes all users that belong to that group from Avaya Spaces.

LDAP group priority order

If a user belongs to multiple LDAP groups that are configured for automatic registration, Avaya Aura® Device Services must choose which settings to use. There might be the following use cases:

- User belongs to multiple LDAP groups with different names.
- User belongs to multiple LDAP groups with the same name. This might occur if the same user is configured on multiple LDAP servers.

User belongs to multiple LDAP groups with different names

Avaya Aura® Device Services sorts all LDAP groups that use the automatic registration functionality in case insensitive ascending alphabetical order and assigns a unique priority number to each LDAP group based on this order. If you have multiple LDAP servers in your deployment, Avaya Aura® Device Services sorts all groups in all servers. If a user belongs to multiple LDAP groups, Avaya Aura® Device Services uses the group settings with the highest priority for that user.

* Note:

Avaya Aura® Device Services sorts groups in case insensitive order.

For example, Avaya Aura® Device Services might assign priorities as follows:

LDAP group	Priority
cn=adminGroup	2
cn=AADSGroup	1
cn=SMGRGroup	4
cn=OtherGroup	3

If a user belongs to cn=OtherGroup and cn=adminGroup groups, Avaya Aura® Device Services will use settings configured for the cn=adminGroup group.

User belongs to LDAP groups with the same name

An enterprise user can be configured on multiple LDAP servers. If the user is a member of groups that have the same name on these servers, Avaya Aura® Device Services determines which settings to use based on the provenance priority configured for each LDAP server on the LDAP Configuration page on the Avaya Aura® Device Services administration portal.

* Note:

For an LDAP group configured for automatic registration, Avaya Aura® Device Services displays the provenance priority and the LDAP server on the LDAP Group Auto Assign page in the **Directory** field.

For example, the user johndoe@aads.example.com is configured on two LDAP servers: OpenLDAP and Active Directory 2016. This user is a member of the cn=adminGroup group on both servers. If the provenance priority is 3 for the OpenLDAP server and 2 for the Active Directory server, then Avaya Aura® Device Services uses settings configured for the cn=adminGroup on Active Directory.

Related links

[Modifying the provenance priority](#) on page 198

Enabling automatic registration for an LDAP group

About this task

When automatic registration is enabled for a group, Avaya Aura® Device Services automatically registers new group users on Avaya Spaces or removes users that are deleted from the group. Avaya Aura® Device Services registers new users with the license, time zone, and language settings that you configured for the group.

If a user that belong to an LDAP group that uses automatic registration was already registered on Avaya Spaces through the Assign License page, Avaya Aura® Device Services overwrites the existing settings with the settings configured for the LDAP group.

You cannot configure automatic registration settings while Avaya Aura® Device Services is synchronizing data with LDAP servers.

Before you begin

- Enable automatic synchronization with your enterprise LDAP server. Avaya Aura® Device Services registers new members of an LDAP group selected for automatic registration on Avaya Spaces when synchronizing data with the LDAP server. If synchronization is disabled, Avaya Aura® Device Services displays a warning message on the LDAP Group Auto Assign page.

For more information about enabling synchronization, see [Setting up user synchronization with the LDAP server](#) on page 202.

- If you are planning to assign Business or Power Avaya Spaces user licenses, ensure that you have enough licenses of the required type.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces > Users and License > LDAP Group Auto Assign**.
2. In the **Search** field, start typing the name of an LDAP group and then press **Enter** to display search results.
3. Select the required LDAP group.
4. From **License**, select an Avaya Spaces license to assign to LDAP group users.

You can select either an Essential, Power, or Business license. Business and Power licenses are only available if your company purchased these license types.

5. **(Optional)** From **Time Zone**, select a time zone for the users of the group.

The list contains time zones available on Avaya Spaces. If you leave this field blank, the default time zone for your Avaya Spaces company is used.

6. **(Optional)** From **Language**, select a language for the users of the group.

The list contains languages available on Avaya Spaces. The default language is English.

7. Do one of the following:

- If you want to keep a user on Avaya Spaces after the user is deleted from the LDAP group, clear the **Delete users removed from the LDAP group from Spaces** check box.
- If you want to remove a user from Avaya Spaces after the user is deleted from the LDAP group, select the **Delete users removed from the LDAP group from Spaces** check box.

8. Click **Register**.

Avaya Aura® Device Services starts registering all users of the LDAP group on Avaya Spaces on the next synchronization with LDAP. Avaya Aura® Device Services displays these users on the Assign License page with the “IN_PROGRESS” status. When the registration completes, Avaya Aura® Device Services displays these users on the View and Manage page.

9. **(Optional)** To start the registration process immediately, perform manual synchronization with your LDAP server:

- Navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
- Select the appropriate LDAP server.
- Click **Force LDAP Sync**.

Updating the automatic registration settings for an LDAP group

About this task

You can modify the following settings that Avaya Aura® Device Services uses when automatically registering LDAP group users on Avaya Spaces:

- License
- Time Zone
- Language

Avaya Aura® Device Services applies changes to all users of the LDAP group that are currently registered on Avaya Spaces.

Before you begin

If you are planning to assign a new Avaya Spaces license type to a group, ensure that you have enough licenses of the required type.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces > Users and License > LDAP Group Auto Assign**.
2. From the list of LDAP groups that use automatic registration, select the check box next to the appropriate group name.
3. Click **Update**.
4. In the LDAP Group Update window, select the appropriate license type, time zone, and language.

5. Click **Update**.

Avaya Aura® Device Services applies changes on the next synchronization with the LDAP server.

6. **(Optional)** To apply changes immediately, perform manual synchronization with the LDAP server.

Disabling automatic registration for an LDAP group

About this task

Use this procedure to disable the automatic registration of users in an LDAP group. When automatic registration is disabled for a group, Avaya Aura® Device Services stops automatically registering new users of that group on Avaya Spaces. All users of that group that are currently registered on Avaya Spaces remain registered.

If a user belongs to other LDAP groups configured for automatic registration, then Avaya Aura® Device Services uses the settings from another group. The settings Avaya Aura® Device Services uses depend on the LDAP group priority.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces > Users and License > LDAP Group Auto Assign**.
2. From the list of LDAP groups that use automatic registration, select the check box next to the appropriate group name.
3. Click **Unregister**.
Avaya Aura® Device Services applies changes on the next synchronization with the LDAP server.
4. **(Optional)** To apply changes immediately, perform manual synchronization with the LDAP server.

Avaya Spaces user management

Avaya Aura® Device Services displays Avaya Spaces users and the licenses assigned to these users on the View and Manage page. On this page, you can perform the following operations for enterprise directory users registered on Avaya Spaces:

- Assign a different license to a user.
- Deallocate an advanced license from a user.
- Delete a user from your Avaya Spaces company.

You cannot delete an Avaya Spaces user using the Avaya Aura® Device Services web administration portal. The user's record remains on Avaya Spaces. You must submit a written request to the Avaya Spaces administrator to delete the user from Avaya Spaces.

* Note:

- You cannot perform any of these operations for users that were created on Avaya Spaces. For these users, Avaya Aura® Device Services displays False in the **From**

LDAP field. To manage users created on Avaya Spaces, use the Avaya Spaces web administration portal.

- You cannot perform any of these operations for a user that belongs to an LDAP group that is configured for automatic registration. For these users, Avaya Aura® Device Services displays the LDAP Group DN in the **Registered GroupDN** field.
- You cannot perform any of these operations when Avaya Aura® Device Services synchronizes data with an LDAP server or Avaya Spaces or performs the Avaya Spaces user audit.

You cannot perform multiple management operations for the same user at the same time. For example, you cannot delete a user if you are assigning a different license for that user.

Avaya Aura® Device Services displays the status information about ongoing management operations in the Status column for each Avaya Spaces user and below the list of Avaya Spaces users. Avaya Aura® Device Services updates this status information approximately every two minutes.

Viewing user information

About this task

On the View and Manage page, the list of Avaya Spaces users contains general user information, such as the first name, last name, and email address. You can open a user entry to view more detailed information, such as the following:

- Time zone
- Language
- Whether the user was created on Avaya Spaces or imported from LDAP
- License type
- Whether the license was updated last on Avaya Aura® Device Services or on Avaya Spaces
- License expiration date
- Phone numbers

When you open a user entry, Avaya Aura® Device Services automatically synchronizes with Avaya Spaces to obtain the latest information for that user.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces > Users and License > View and Manage**.

Avaya Aura® Device Services displays the list of Avaya Spaces users.

2. Navigate to the required user and double-click the user entry to open it.

Avaya Aura® Device Services displays a separate window with the detailed user information.

Deallocating licenses

About this task

You have a limited number of advanced Business or Power licenses for Avaya Spaces. Therefore, the number of licenses might be less than the number of users in your deployment. If required,

you can deallocate an advanced license from a user and reassign it to another Avaya Spaces user. When you deallocate a license from a user, Avaya Spaces assigns the Essential license to that user.

This procedure is intended for users for enterprise users registered on Avaya Spaces. To deallocate a license from a user created on Avaya Spaces, use the Avaya Spaces web administration portal.

You cannot deallocate a license from a user that belongs to a LDAP group, which is configured for automatic registration of group users. You cannot deallocate Essential and Trial licenses.

You cannot deallocate licenses when Avaya Aura® Device Services synchronizes data with an LDAP server or Avaya Spaces or performs the Avaya Spaces user audit.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces > Users and License > View and Manage**.
2. Do one of the following:
 - To deallocate a license from a single user, select the check box next to the user's name.
 - To deallocate licenses from multiple users, select the check boxes for the required users.
 - To deallocate licenses from all users, select the check box in the table header.
3. Click **De-Allocate**.

Result

Avaya Aura® Device Services starts the deallocation process and displays its status in the Status column. Depending on the number of users, this process might take several minutes to complete. Avaya Aura® Device Services notifies you when the process is completed.

Related links

[Avaya Spaces user management operation fails](#) on page 425

Assigning a different license to Avaya Spaces users

About this task

Use this procedure to assign licenses of another type to enterprise users registered on Avaya Spaces. You can assign a new license to a single user or to multiple users at the same time.

Avaya Aura® Device Services notifies you if the license that you want to assign to a user has expired or is expiring soon. You can assign a license to a user even if the license has expired. In this case, the Essential license will be assigned to the user.

If a user has a Trial license of any type assigned, you can assign either a Business or Power license to the user. You cannot assign an Essential license to a user with a Trial license.

If you assign a Business or Power license to a user with an Essential or Trial license, you can cancel this operation from the Assign License page until Avaya Aura® Device Services assigns a new license to the user. In this case, the user's status is displayed as "UDPATE_CANCELLED" on the View and Manage page.

You cannot assign a new license to a user that belongs to a LDAP group, which is configured for automatic registration of group users. You also cannot assign a new license to a user created on Avaya Spaces. To assign a new license to a user created on Avaya Spaces, use the Avaya Spaces web administration portal.

You cannot assign new licenses when Avaya Aura® Device Services synchronizes data with an LDAP server or Avaya Spaces or performs the Avaya Spaces user audit.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces > Users and License > View and Manage**.
2. Do one of the following:
 - To update a license for a single user, select the check box next to the user's name.
 - To update licenses for multiple users, select the check boxes for the required users.
 - To update licenses for all users, select the check box in the table header.
3. Select the check box for the users you want to update.
4. Click **Update**.
Avaya Aura® Device Services displays the Update Users License window.
5. Do one of the following:
 - To assign a license to each user separately, in **Update License**, select the required license type for each user.
 - To assign the same license to all users, select the **Bulk Update** check box and then select the required license type from **Select License**.
6. Click **Save**.
7. In the Confirm Action window, click **OK**.

Result

Avaya Aura® Device Services starts the update process and displays the update status in the Status column. Depending on the number of users, the update process might take several minutes to complete.

Related links

[Avaya Spaces user management operation fails](#) on page 425

[Cancelling user registration and license upgrade operations](#) on page 178

Removing users from your Avaya Spaces company

About this task

You can remove from Avaya Spaces those enterprise directory users that were registered on Avaya Spaces using the Avaya Aura® Device Services web administration portal.

When you delete an enterprise directory user that was registered on Avaya Spaces, this user is *not* removed from the enterprise directory. You can re-register this user on Avaya Spaces in the future.

You cannot remove users when Avaya Aura® Device Services synchronizes data with an LDAP server or Avaya Spaces or performs the Avaya Spaces user audit.

 Note:

- To remove users that were created on Avaya Spaces, use the Avaya Spaces web administration portal.
- You cannot remove a user that belongs to an LDAP group, which is configured for automatic registration of group users.
- After you perform this procedure, the user's record remains on Avaya Spaces. To completely delete a user and all associated records from Avaya Spaces, you must send a written request to the Avaya Spaces administrator.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces > Users and License > View and Manage**.
2. Do one of the following:
 - To remove a single user, select the check box next to the user's name.
 - To remove multiple users, select the check boxes for the required users.
 - To remove all users, select the check box in the table header.
3. Click **Delete**.
4. In the Confirm Action window, click **OK**.

Result

Avaya Aura® Device Services starts the removal process and displays its status in the Status column. Depending on the number of users, this process might take several minutes to complete. Avaya Aura® Device Services notifies you when users are removed from your company in Avaya Spaces.

Related links

[Avaya Spaces user management operation fails](#) on page 425

Performing an Avaya Spaces user audit

About this task

In some cases, the Avaya Aura® Device Services and Avaya Spaces databases might contain different information about a user. For example, if you cancel a license assignment operation, Avaya Aura® Device Services and Avaya Spaces might contain different information about the user license. To identify and resolve these differences, you can use the audit operation.

The audit verifies the following:

- Whether the user exists on both Avaya Aura® Device Services and Avaya Spaces.
- Whether the user has the same license type on both Avaya Aura® Device Services and Avaya Spaces.

The audit does not verify other user attributes, such as the first name, last name, or email address.

To fix inconsistencies between databases, the audit process uses information from the Avaya Aura® Device Services database, unless the user exists on Avaya Spaces only. In this case, you can choose which database record to use. The audit process does not remove users from Avaya Aura® Device Services.

Important:

For users originally created on Avaya Spaces (non-LDAP users), you cannot fix inconsistencies between databases by adding or removing these users from Avaya Spaces. For example, if the audit identified that a non-LDAP user exists in the Avaya Aura® Device Services but does not exist in the Avaya Spaces database, then you can only delete the user from Avaya Aura® Device Services.

You cannot perform the audit at the same time as another user management operation, such as adding or deleting a user or updating licenses. During the audit, you cannot perform user management operations on the Assign License and View and Manage pages.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces > Users and License > View and Manage**.

2. Click **Audit Scan**.

Avaya Aura® Device Services displays the list of users whose Avaya Aura® Device Services and Avaya Spaces database records do not match. For more information about audit scan results, see [Audit status](#) on page 177.

3. From **Action for Users not in AADS**, select one of the following options to process users that exist on Avaya Spaces only:

- **ADD on AADS:** To create these users on Avaya Aura® Device Services.
- **DELETE from SPACES:** To remove these users from Avaya Spaces.

Avaya Aura® Device Services displays actions that Avaya Aura® Device Services will perform to fix inconsistencies between Avaya Aura® Device Services and Avaya Spaces databases in the Post Submit Action column.

4. Click **Submit**.

Avaya Aura® Device Services starts processing all records found during the scan process.

Audit status

The following table shows data mismatch types that Avaya Aura® Device Services can display for users found during the audit scan process.

Data mismatch type	Description	Action	Action performed automatically
USER_NOT_IN_AADS	The user exists on Avaya Spaces only and does not exist on Avaya Aura® Device Services.	The following options are available: - Add the user to Avaya Aura® Device Services. - Remove the user from Avaya Spaces.	No, you must select the action
USER_NOT_IN_SPACES	The user exists on Avaya Aura® Device Services only and does not exist on Avaya Spaces.	The user that exists on Avaya Aura® Device Services is created on Avaya Spaces.	Yes
LICENSE_MISMATCH	The user has different licenses on Avaya Aura® Device Services and Avaya Spaces.	The license information on Avaya Spaces is updated according to the license information from the Avaya Aura® Device Services database.	Yes

Cancelling user registration and license upgrade operations

About this task

You can cancel the following operations:

- Enterprise user registration on Avaya Spaces.
- Upgrade of Essential or Trial licenses to Business or Power licenses.

You cannot cancel an operation for a user if this user belongs to a LDAP group that is configured for automatic registration.

When you cancel a user registration or license upgrade operation, Avaya Aura® Device Services keeps all users that were not processed on the Assign License page and assigns the “CANCELLED” status to these users. If Avaya Aura® Device Services processed any users before cancellation, these users are displayed on the View and Manage page.

If you cancel a user registration operation, you can repeat the registration process later.

If you cancel the license upgrade operation for a user, you can either confirm cancellation or resume the operation from the Assign License page. Until then, the user’s status is displayed as “UPDATE_CANCELLED” on the View and Manage page.

Important:

After cancelling an operation, you must perform an audit from the View and Manage page to ensure that user information is properly synchronized between Avaya Aura® Device Services and Avaya Spaces.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces > Users and License > Assign License**.
2. Click **Cancel** to cancel a user registration or license upgrade process.

The **Cancel** button is only enabled if any of users on the Avaya Spaces have either the "IN_PROGRESS" or "TO_BE_PROCESSED" status.

3. If you cancelled the license upgrade operation for a user, do the following to confirm cancellation:
 - a. Select the user from the table on the Assign License page.
 - b. Click **Delete**.

Next steps

Perform the audit operation as described in [Performing an Avaya Spaces user audit](#) on page 176.

Related links

[Registering enterprise users on Avaya Spaces](#) on page 166

[Assigning a different license to Avaya Spaces users](#) on page 174

Updating Avaya Spaces integration parameters

About this task

After Avaya Spaces integration is configured, you can update Avaya Spaces integration parameters.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces > Configuration**.
2. Update the following parameters as appropriate:
 - **Spaces API Key**
 - **Spaces API Key secret**
 - **Spaces URI**
3. Click **Save**.

Related links

[Avaya Spaces integration settings](#) on page 179

Avaya Spaces integration settings

From the Configuration page, you can update the following Avaya Spaces parameters without having to reconfigure integration with Avaya Spaces:

Setting	Notes
Spaces API Key	You can use any API key and API key secret that belong to the company with which you set up integration.  Important: If you want to set up integration for another company, you must delete the existing configuration first. If you provide an API key or API key secret for another company in the existing configuration and save the configuration, Avaya Aura® Device Services displays an error message.
Spaces API Key secret	
Spaces URI	You do not need to reconfigure integration if Avaya Spaces only changes its URI and other company data remains unchanged. For example, when Avaya Spaces migrates to another URI.

Related links

[Updating Avaya Spaces integration parameters](#) on page 179

Disabling Avaya Spaces integration

About this task

Use this procedure to disable integration with Avaya Spaces. When you disable integration, Avaya Aura® Device Services does not synchronize user data with the company you used for integration. You also cannot use the Avaya Aura® Device Services web administration portal to manage Avaya Spaces users or licenses for that company.

When integration is disabled, the Avaya Spaces configuration data remains on Avaya Aura® Device Services, so you can re-enable integration in the future.

Procedure

1. On the Avaya Aura® Device Services administration portal, navigate to **Spaces > Configuration**.
2. Clear the **Enable Spaces Integration** check box.
3. In the Confirmation window, click **OK**.
4. When the process is completed, click **OK** again.

Deleting the Avaya Spaces configuration

About this task

Use this procedure to delete the Avaya Spaces configuration data from Avaya Aura® Device Services. If you want to enable integration in the future, you will need to set it up again.

You must delete the existing configuration if you want to set up integration for another company. Avaya Aura® Device Services only supports integration with one company at a time.

Procedure

1. On the Avaya Aura® Device Services administration portal, navigate to **Spaces > Configuration**.
2. Click **Delete**.
3. In the Confirmation window, click **OK**
4. After the deletion process is completed, click **OK** again.

Related links

[Configuring data synchronization between Avaya Aura Device Services and Avaya Spaces](#) on page 158

Viewing the Avaya Spaces connection status

About this task

After you set up integration with Avaya Spaces, Avaya Aura® Device Services checks the connection to Avaya Spaces periodically and displays the connection status on the Configuration page. If Avaya Aura® Device Services cannot connect to Avaya Spaces, it displays an error message, which you can use to fix the connection issue.

Avaya Aura® Device Services checks the connection status every one hour. If disconnected from Avaya Spaces, Avaya Aura® Device Services checks the connection status every five minutes.

Procedure

1. On the Avaya Aura® Device Services administration portal, navigate to **Spaces > Configuration**.
2. In the Status area, view the connection status.

Related links

[Avaya Aura Device Services alarms list](#) on page 342

[Avaya Spaces connectivity errors](#) on page 422

Configuring Avaya Spaces SSO for Avaya Spaces clients

About this task

With the Avaya Spaces SSO functionality, Avaya Spaces clients can use features available through Avaya Aura® Device Services REST APIs, such as dynamic configuration or contact search in Avaya Aura® directories. Avaya Spaces clients use Avaya Spaces SSO Bearer tokens to authenticate on Avaya Aura® Device Services REST APIs.

When Avaya Spaces SSO is disabled, Avaya Aura® Device Services REST API features are unavailable for Avaya Spaces clients.

This procedure applies to Avaya-provided clients, such as Avaya Spaces Calling browser extension, and to your own custom Avaya Spaces clients.

Before you begin

Configure your company and domain on Avaya Spaces.

Procedure

1. On the Avaya Aura® Device Services administration portal, navigate to **Spaces > Spaces SSO**.
2. Select the **Enable SSO** check box.
3. In **Domain**, type the name of the domain configured for your company in Avaya Spaces and click **Add**.
4. If you have multiple domains configured for your company in Avaya Spaces, repeat the previous step for all these domains.
5. If you are configuring Avaya Spaces SSO for your own web client, do the following:
 - a. In **Client ID**, enter the ID of your web client.
 - b. Click **Add**.

This step is not required for the Avaya Spaces Calling browser extension because Avaya Aura® Device Services already contains information about its ID.

6. Click **Save**.

Chapter 6: LDAP server management

You must configure the enterprise LDAP server to authenticate the users and administrators of Avaya Aura® Device Services. The LDAP Configuration screen on the Avaya Aura® Device Services web administration portal displays the enterprise LDAP server that you configured during deployment.

You cannot perform all LDAP server management tasks with the configuration utility. Use the Avaya Aura® Device Services web administration portal to do the following:

- Configure multiple LDAP directories.
- Specify an order in which Avaya Aura® Device Services accesses LDAP directories.
- Select which LDAP directories are used for authentication.
- Configure multiple base context Distinguished Names (DNs).
- Set up LDAP synchronization.
- Configure attribute mappings.

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 235.
- If FIPS is enabled on Avaya Aura® Device Services, you must use the secure LDAP (LDAPS) connection to access LDAP servers.
- If you are using more than one LDAP, use different domains instead of the same domain.
- In an Avaya Aura® environment, after creating or updating a user in System Manager, you must force LDAP synchronization or wait 24 hours for your changes to take effect.

Related links

[Updating user attributes in LDAP](#) on page 208

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**.

Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.

2. For each LDAP server configured on Avaya Aura® Device Services, 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 184.

Procedure

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

Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.

Enterprise LDAP Server Configuration

ActiveDirectory_2012 **ActiveDirectory_2016**

Configure the Enterprise LDAP server in order to authenticate Avaya Aura Device Services users and administrators.

Enterprise-Directory Type: **ActiveDirectory_2012** ☒ Use for authentication ☒ Use for contact search

Provenance Priority: **1** Authentication Domain: **gsc.com** ☐ Edit Domain ☒ Enable DNS

Server Address and Credentials

Secure LDAP: ☐

*Address: **_ldap_tcp.gsc.com** *Port: **3268**

*Bind DN: **gsc\Administrator** *Bind Credential: **.....**

Base Context DN: **ou=uc-smgr7,dc=gsc,dc=cor** *UID Attribute ID: **mail**

☐ Use additional Base Context DN: *Role Filter: **(&(objectClass=group)(meml**

*Role Attribute ID: **cn**

Roles Context DN: **ou=uc-smgr7,dc=gsc,dc=cor** Role Name Attribute:

Role Attribute is DN: **false** Allow Empty Passwords: **false**

Search Scope: **Subtree** Role Recursion: **false**

Administrator Role: **ADMINS** User Role: **USERS**

Auditor Role: Services Administrator Role:

Services Maintenance and Support Role: Security Administrator Role: **ADMINS**

Language used in Directory: **English (en)**

Active Users Search Filter: Last Updated Time Attribute ID: **modifyTimestamp**

Users Search Additional Filter: **(objectClass=inetOrgPerson)**

User Synchronization Update Instructions

Last Sync Status : **Successful** as on : **Thu, Feb 11, 2021 11:22:40 (UTC+3)**

2021-02-07 **11:00** **AM** (UTC+3)

2. Click the plus (+) icon.

Avaya Aura® Device Services 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. Specify the method Avaya Aura® Device Services uses to discover the LDAP server:
 - To discover the LDAP server using DNS SRV entries, select the **Use DNS** check box and in **Address** specify the name of a domain for which you want to discover LDAP servers.
 - To discover the LDAP server using the server IP address or FQDN, clear the **Use DNS** check box and specify the IP address or FQDN in the **Address** field.

For more information about these attributes, see [Enterprise LDAP Server Configuration field descriptions](#) on page 186. For more information about LDAP server discovery using DNS SRV records, see [LDAP server discovery using DNS SRV records](#) on page 194.

6. 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 186.

7. 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**.
8. If you want to use the new server for contact search, select the **Use for contact search** check box.
9. Click **Save**.

Next steps

For each LDAP server configured on Avaya Aura® Device Services, set up a provenance priority order.

Related links

[Modifying the provenance priority](#) on page 198

Enterprise LDAP Server Configuration field descriptions

Name	Description
Enterprise-Directory Type	Specifies the name of the enterprise directory. The options are: • ActiveDirectory_2012 • ActiveDirectory_2016 • ActiveDirectory_2019 • ActiveDirectory_2022 • ActiveDirectory_2025 • Azure Active Directory • Domino 7.0 or 8.5.3 • LDS_2012 • Novell 8.8 • OpenLDAP 2.4.44 and 2.4.46 • OracleDirectoryServer 11.1.1
Provenance Priority	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 directory value with higher provenance priority is returned. For example, if firstName is obtained from two

Name	Description
	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.

Server Address and Credentials

Name	Description
Use for authentication	Specifies whether the server is used for authentication and authorization. If OAuth is enabled, you can select or clear this check box after installation. If OAuth is enabled, but this check box is not selected, then you can only log in to the Avaya Aura® Device Services web administration portal using the credentials of the administrative user created during OVA installation.
Use for Contact Search	Specifies whether this LDAP server is used for the contact search. If you use the onboard OpenLDAP server, this option is enabled by default.
Use DNS	Specifies whether Avaya Aura® Device Services uses DNS SRV records to discover the LDAP server. • If the check box is selected, Avaya Aura® Device Services uses the domain name specified in the Address field to discover all LDAP servers associated with this domain name in DNS SRV records. • If the check box is not selected, Avaya Aura® Device Services uses the IP address or FQDN specified in the Address field to discover the LDAP server.
Secure LDAP	Indicates whether the LDAP server connection is secure or not. If FIPS is enabled, you must use the secure LDAP connection to access LDAP servers. If you are using a secure LDAP connection, you must also import the LDAP server trusted certificate to Avaya Aura® Device Services.
Import Certificate	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. You cannot import a certificate if: • The certificate contains an unsupported critical extension. • The certificate expired. • The start date of the certificate is in the future.
Windows Authentication	Specifies whether to use Windows Authentication.

Name	Description
	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.
Address	Specifies the address of the LDAP server. The exact value depends on the value of the Use DNS field as follows: • If the Use DNS check box is not selected, provide the IP address or FQDN of the LDAP server. If you use the secure LDAP connection (LDAPS), you must use the LDAP server FQDN. IP addresses are not supported. If the LDAP server uses IPv6, use the LDAP server FQDN. • If the Use DNS check box is selected, provide a domain name. Avaya Aura® Device Services uses this domain name to discover all LDAP server instances associated with this domain name in DNS SRV records. If multiple LDAP server instances are discovered, Avaya Aura® Device Services determines a LDAP server to connect to based on the priority and weigh settings configured in SRV records. Use the following format: <pre><code>_<SERVICE>._tcp.<DOMAIN_NAME>.</code></pre> In this entry, <code><SERVICE></code> is <code>ldap</code> if you use the standard LDAP connection, or <code>ldaps</code> if you use the secure LDAP connection. For example: <code>_ldap._tcp.example.com.</code> If you use this option, you must also ensure that: - The <code>/etc/resolv.conf</code> file contains the specified domain name in the “search” or “domain” entry. - All DNS servers listed in the <code>/etc/resolv.conf</code> for the domain name contain SRV records for all appropriate LDAP server instances. This field is mandatory.
Port	Specifies the port of the LDAP server.  Important: 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

Name	Description
	attribute is not replicated to the global catalog. You must manually add all required attributes in the global catalog attributes list. This field is mandatory.
Bind DN	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. The format of the Bind DN depends on the configuration of the LDAP server. This field is mandatory.  Note: 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. For example: for Active Directory, you can use <code>domain\user</code>, <code>user@domain</code>, as well as the actual DN of the user object.
Bind Credential	Specifies the password of the administrative user. The maximum password length depends on the LDAP server type that you use in your deployment. The supported characters are: • Lowercase letters: a to z • Uppercase letters: A to Z • Numerics: 0 to 9 • Special characters are supported
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, <code>dc=domain, dc=company, dc=com</code>. If you are using multiple authorization domains, Avaya recommends including a domain component to the Base Context DN. For example, <code>dc=avaya, dc=com</code>.  Note: Some LDAP sources, such as Domino, typically do not contain the domain component in Base Context DN. For example, <code>o=MyCompany</code>. If Base Context DN does not contain the domain component, Avaya Aura® Device Services considers them “empty” Base Context DN 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 DN.

Name	Description
Use additional Base Context DN	Enables Avaya Aura® Device Services contact search and quick search. 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. You can configure up to 10 additional Base Context DNs. If you select this check box, you can see the View/Edit button. Auto-configuration will use only the primary base context DN.
View/Edit	Enables access to the Addition Base DN Configuration page, where you can add or delete additional Base Context DNs.
UID Attribute ID	Specifies the unique attribute of the user on LDAP, which is used to search for users in the LDAP server. If you are using multiple authentication domains, you must use one of the following values: • mail • userPrincipalName • Any custom attribute that uses a domain-qualified value If you are not using multiple authentication domains, you must use one of the following values: • uid, if you use OpenLDAP • sAMAccountName • mail • userPrincipalName This field is mandatory.  Note: When the UID attribute is set to “mail” on OpenLDAP, use Apache Directory Studio to set the email value for the OpenLDAP administrative user. This enables the administrative user to log in to the Avaya Aura® Device Services web administration portal using their email.
Role Filter	Specifies the search filter used to search the role of the user. For example, (&(objectClass=group) (member={1}))
Role Attribute ID	Specifies that the user is a member of the groups defined by that attribute. For example, objectCategory This field is mandatory.
Roles Context DN	Specifies the complete Distinguished Name (DN) to search for a user role, that is, for Role Filter.

Name	Description
	For example, dc=domain,dc=company,dc=com
Role Name Attribute	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.
Role Attribute is DN	Indicates whether the role attribute of the user contains DN. The default value is true.
Allow Empty Passwords	Indicates whether LDAP Server acknowledges the empty password. The default value is false.
Search Scope	Specifies the search level in the LDAP hierarchy. The options are: • Object: For searching only for the object. • One Level: For including one level in the LDAP hierarchy in the search. • Subtree: For including subtree in the LDAP hierarchy in the search. The default value is Subtree.
Role Recursion	Specifies whether role recursion is enabled. The options are: • true • false If your LDAP configuration includes nested groups, you can set the Role Recursion parameter to <code>true</code> so that Avaya Aura® Device Services computes role membership by searching through LDAP structures recursively. For example, the user jsmith can be in the Sales group, which can be in the AADS users group. In this case, Role Recursion must be set to true for jsmith to be recognized as a member of the AADS users group. If you set this parameter to <code>false</code>, Avaya Aura® Device Services does not compute the role membership information recursively.  Note: Certified with 300 nested groups with 2 levels for each user.
Administrator Role	Specifies the administrator role in which the administrative users are assigned.
Security Administrator Role	Specifies the security administrator role in which the administrative users can manage web certificates from the web administration portal.
User Role	Specifies the user role in which the common users are assigned.
Auditor Role	Specifies the auditor role in which the users can audit the system.

Name	Description
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 those 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: <code>(&(objectClass=user)(objectCategory=Person))</code>.
Last Updated Time Attribute ID	Specifies when the user is updated on LDAP. The exact value depends on the LDAP server type that you use. Avaya recommends that you use the following values: • For Active Directory: <code>whenChanged</code>. • For OpenLDAP: <code>modifyTimestamp</code>. This field is mandatory.

Configuration for Windows Authentication

Name	Description
Service Principal Name (SPN)	Specifies the service principal name UIDAttributeID must be userPrincipalName.
Import keytab file	Imports the <code>tomcat.keytab</code> file and overwrites the existing file.
Kerberos Realm	Specifies the Kerberos realm.
DNS Domain	Specifies the DNS domain of the Domain Controller.
KDC FQDN	Specifies the FQDN of the Domain Controller.
KDC Port	Specifies the port number. The default KDC port is 88.

Button	Description
Test Connection	Tests the connection changes.
Save	Saves the changes made to the enterprise directory.
Modify Attribute Mappings	Modifies the attributes of the LDAP server.

Configuring additional base context DNs

About this task

Use this procedure to add additional base context DNs. Base context DNs are used to specify sections of the LDAP directory where LDAP searches for:

- Contacts, when performing LDAP lookups. The use of multiple base context DNs ensures maximum search performance.
- Groups, when configuring and publishing settings using the Dynamic Configuration service.

You can add up to 10 base context DNs for one LDAP source.

You can also use an additional base context DN for authentication. In this case, this additional base context DN uses the role context DN that is configured in the primary LDAP server. You can use only the primary domain or its sub-domains as an authentication domain.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.
2. Select the appropriate LDAP server.
3. In the Server Address and Credentials section, select the **Use additional Base Context DN** check box and then click **View/Edit**.
4. In the Additional Base Context DN Configuration window, click **+**.
5. In the table, click the **Base Context DN** field and then 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. If you want to use the base context DN for contact search, select the **Use for contact search** check box.
8. Click **Save**.
9. In the Server Address and Credentials section, click **Save**.

LDAP server discovery using DNS SRV records

From Release 8.1.5, you can configure Avaya Aura® Device Services to discover LDAP server instances using DNS SRV records. With this functionality, you do not need to explicitly provide the IP address or the FQDN of an LDAP server. Instead, provide a domain name, and Avaya Aura® Device Services uses DNS SRV records to discover all LDAP server instances associated with this domain name. Avaya Aura® Device Services supports this functionality for both LDAP and LDAPS protocols.

The advantage of using DNS SRV records is that you can specify multiple LDAP server instances in SRV records, and Avaya Aura® Device Services discovers all these instances automatically. For example, if you use primary and backup LDAP servers, and the primary LDAP server instance goes offline, Avaya Aura® Device Services will automatically discover and connect to the secondary LDAP server. If you do not use DNS SRV records and explicitly specify the FQDN or IP address of the primary LDAP server, Avaya Aura® Device Services cannot discover the secondary LDAP server instance. You must manually update the LDAP server IP address or FQDN on the Avaya Aura® Device Services web administration portal.

The following is a high-level workflow that Avaya Aura® Device Services performs to discover LDAP servers using DNS SRV records:

1. Obtains the domain name from the LDAP server configuration.
2. Uses the `/etc/resolv.conf` file to determine which DNS servers listed in this file are associated with the domain name.
3. Obtains SRV records for all LDAP servers associated with the domain name and uses these records to obtain FQDNs and port numbers of the LDAP servers.
4. If a single SRV record is found, Avaya Aura® Device Services connects to the LDAP server specified in this record.

If multiple SRV records are found, Avaya Aura® Device Services uses the priority and weight values specified in the SRV records to determine a LDAP server to connect. Avaya Aura® Device Services connects to a LDAP server with the lowest priority value. If multiple servers have the same priority, Avaya Aura® Device Services connects to a server with the higher weight value.

For information about the actions required to set up LDAP server discovery using DNS SRV records, see [Checklist for configuring LDAP discovery using DNS SRV records](#) on page 195.

DNS SRV record overview

DNS SRV record is a record on a DNS server that defines the location of a service, such as LDAP, for a specific domain. You must provide a separate DNS SRV record for each LDAP server instance that must be discoverable using SRV lookup. If you have multiple LDAP server instances, you must create a separate DNS SRV record for each instance.

A DNS SRV record for a LDAP server uses the following format:

```
_<SERVICE>._tcp.<DOMAIN_NAME> IN SRV <PRIORITY> <WEIGHT> <PORT>  
<LDAP_FQDN>
```

In this entry:

- **SERVICE** is one of the following symbolic names for the LDAP service:
 - If you use the standard LDAP connection: `ldap`
 - If you use the secure LDAP (LDAPS) connection: `ldaps`
- **DOMAIN_NAME** is the domain name for which this SRV record applies. The domain name must end with a dot.
- **PRIORITY** is the priority of the LDAP server. Lower the value means higher the priority.
- **WEIGHT** is the relative weight of the record. This parameter is used if two or more records have the same priority. Higher the value means higher the relative weight of the LDAP server.
- **PORT** is the port to access the LDAP server.
- **LDAP_FQDN** is the FQDN of the LDAP server. The FQDN must end with a dot.

If you use multiple DNS servers, each DNS server must have the same SRV records for LDAP server instances.

For example, if your domain name is `example.com`, and you have a primary LDAP server, which FQDN is `primary_ldap.example.com`, and a secondary LDAP server, which FQDN is `backup_ldap.example.com`, you can configure DNS SRV records on your DNS servers as follows:

```
_ldap._tcp.example.com. IN SRV 10 100 389 primary_ldap.example.com.
_ldap._tcp.example.com. IN SRV 20 100 389 backup_ldap.example.com.
```

For more information about configuring SRV records on a DNS server, see the documentation for the DNS server you use in your deployment.

Checklist for configuring LDAP discovery using DNS SRV records

The following checklist lists the configuration tasks you must perform to set up LDAP discovery using DNS SRV records.

No.	Task	Notes	✓
1	If you use the secure LDAP connection, ensure that the Subject Alternative Name of the LDAP certificate contains FQDNs of all LDAP server instances that must be discoverable using SRV lookup.	You can use the following <code>openssl</code> command in the CLI to verify the certificate content: <pre>openssl s_client -connect <ldap server:port> openssl x509 -noout -text</pre> If the Subject Alternative Name does not contain the required FQDNs, reissue the LDAP certificate.	
2	Ensure that the <code>/etc/resolv.conf</code> file contains the appropriate domain name and DNS server addresses.	Ensure that the <code>/etc/resolv.conf</code> file contains the following information: • The name of the domain, for which Avaya Aura® Device Services must	

No.	Task	Notes	✓
		perform LDAP server discovery using DNS SRV records. The list of DNS servers containing DNS SRV records for the LDAP servers. For example, if you want to use DNS SRV records to discover LDAP servers for the example.com domain and use DNS servers with 198.51.100.2 and 203.0.113.5 IP addresses, the <code>/etc/resolv.conf</code> file might look as follows: <pre>search example.com nameserver 198.51.100.2 nameserver 203.0.113.5</pre>	
3	Configure SRV records for LDAP server instances on DNS servers.	On DNS servers listed in the <code>/etc/resolv.conf</code> file, you must create a separate SRV record for each LDAP server instance that must be discoverable. For more information about DNS SRV records, see DNS SRV record overview on page 194. For more information about configuring an SRV record on a DNS server, see the documentation for the DNS server you use in your deployment.	
4	Configure LDAP server settings on the Avaya Aura® Device Services web administration portal.	See Configuring LDAP server discovery using DNS SRV records on page 196.	

Configuring LDAP server discovery using DNS SRV records

About this task

Avaya Aura® Device Services can discover your LDAP server instances using DNS SRV lookup. On the Avaya Aura® Device Services web administration portal, you can provide a domain name instead of an IP address or FQDN of the LDAP server. Avaya Aura® Device Services discovers all available LDAP server instances associated with this domain using SRV records.

Avaya Aura® Device Services determines which LDAP server to use based on the priority and weight configured in SRV records for the servers.

Before you begin

- Ensure that a “search” or “domain” entry of the `/etc/resolv.conf` file contains the domain name for which you want to discover LDAP server instances.

- On your DNS servers specified in the `/etc/resolv.conf` file, configure SRV records for each LDAP server that needs to be discoverable using SRV records. If you have multiple LDAP servers instances, configure an SRV record for each LDAP server instance.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
2. Select the appropriate LDAP server.
3. Select the **Use DNS** check box.
4. In **Address**, type the following:

```
_<SERVICE>._tcp.<DOMAIN_NAME>
```

In this entry:

- `<SERVICE>` is one of the following symbolic names for the LDAP service:
 - `ldap`: If you use the standard LDAP connection to the LDAP server.
 - `ldaps`: If you use the secure LDAP connection to the LDAP server.
- `<DOMAIN_NAME>` is the domain name for which you want to discover LDAP server instances.

For example, if you use the secure LDAP connection to the server and the domain name is `example.com`, type the following:

```
_ldaps.tcp.example.com
```

5. Click **Save**.

Next steps

Test the connectivity to the LDAP server.

Testing connection to an LDAP server

About this task

Use this procedure to ensure that you configured an LDAP server correctly and that Avaya Aura® Device Services can connect to the LDAP server.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.
2. Select the appropriate LDAP server.
3. Click **Test Connection**.

4. If the test fails, check the configured LDAP address FQDN, port, and protocol and run the test again.

Modifying the provenance priority

About this task

If you configured multiple LDAP servers, use this procedure to specify the order in which Avaya Aura® Device Services accesses LDAP directories. For example, if a givenName attribute is defined in two LDAP servers for a given user, the value that Avaya Aura® Device Services uses is based on the order you define.

Procedure

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

Related links

[Starting or stopping Avaya Aura Device Services](#) on page 31
[LDAP group priority order](#) on page 169

Administering the LDAP server configuration

Procedure

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

3. Modify the details of the enterprise directory.
4. Click **Save**.

Related links

[Enterprise LDAP Server Configuration field descriptions](#) on page 186

Enabling LDAP authentication for OAuth

About this task

Use this procedure if you want to use LDAP authentication when OAuth is enabled.

If OAuth is enabled and LDAP authentication is disabled, then you can only log in to the Avaya Aura® Device Services web administration portal using the credentials of the administrative user created during OVA installation.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
2. Select the appropriate LDAP server.
3. Select the **Use for authentication** check box.
4. Click **Save**.

Modifying enterprise directory attribute mappings

About this task

Each LDAP directory type includes a set of pre-defined attributes mappings, which map user attributes that Avaya Aura® Device Services uses to LDAP attributes defined in the default LDAP schema for the respective LDAP directory type. If you use a custom LDAP schema for your LDAP directory type, you must customize the attribute mapping accordingly.

Avaya Aura® Device Services search results do not include attributes that are not mapped to LDAP attributes.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.
2. Select the appropriate LDAP server.
3. In the Server Address and Credentials section, click **Modify Attribute Mappings**.

Avaya Aura® Device Services displays the Enterprise Directory Mappings page. The Modify LDAP Attribute Mappings table contains the following columns:

- Application Field Name contains user attributes that Avaya Aura® Device Services uses.
 - Directory Field Name contains pre-defined attributes from the standard LDAP schema.
 - Custom Field Name enables you to enter custom attribute names.
- In the Modify LDAP Attribute Mappings section, do one of the following for the required attribute:
 - To select one of the pre-defined LDAP attributes, click the **Directory Field Name** cell and then select the required LDAP attribute from the list.
 - To use a custom LDAP attribute, click the **Custom Field Name** cell and enter the name of the required custom LDAP attribute.
 - To un-map the attribute, clear the **Custom Field Name** value and set **Directory Field Name** to **Choose Attribute**.
 - (Optional)** If you want to reset the attribute mapping to its default settings, click **Reset**.
 - Click **Save**.

Avaya Aura® Device Services restarts to apply changes.

Example

The following image shows an Active Directory 2012 attribute mapping example, where:

- Alias and ASCIIGivenname attributes use default mapping.
- ASCIIDisplayname attribute is mapped to the custom asciiDisplayName LDAP attribute.
- ASCIISurname is not mapped to any LDAP attribute

Modify LDAP Attribute Mappings

Application Field Name	Directory Field Name	Custom Field Name
Alias	cn	
ASCIIDisplayname	Choose Attribute	asciiDisplayName
ASCIIGivenname	givenName	
ASCIISurname	Choose Attribute	

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**.

Avaya Aura® Device Services 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> /ptype KRB5_NT_PRINCIPAL /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_spn_user@EXAMPLE.COM /princ HTTP/
aads.example.com@EXAMPLE.COM /ptype KRB5_NT_PRINCIPAL /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.

Selecting an authentication domain

About this task

You can select a domain that the LDAP server uses to authenticate users. For example, if the domain part of the email address does not match the base context DN configuration, you can provide the required domain value instead of the value configured by default.

Procedure

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

Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.

2. Select the appropriate LDAP server.
3. Select the **Edit Domain** check box.
4. In **Authentication Domain**, type the required domain name.
5. Click **Save**.

Avaya Aura® Device Services restarts to apply changes.

Setting up user synchronization with the LDAP server

About this task

Use this procedure to synchronize user data between Avaya Aura® Device Services and a specific LDAP server. Avaya Aura® Device Services synchronizes data that is used for number and email-to-number resolution. You can schedule the synchronization process to occur hourly, daily, or weekly.

You must enable synchronization with the LDAP server if you are planning to use automatic registration of LDAP group users for Avaya Spaces integration. Avaya Aura® Device Services

registers new members of an LDAP group selected for automatic registration on Avaya Spaces when synchronizing data with the LDAP server.

*** Note:**

- When Avaya Aura® Device Services synchronizes data with the LDAP server, the Avaya Spaces user management functionality on the Assign License and View and Manage pages is unavailable.
- If synchronization with the LDAP server fails, Avaya Aura® Device Services displays the “Failed” synchronization status and writes information about the error to the `AADS.log` file.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.
2. Select the appropriate LDAP server.
3. In the User Synchronization Update Instructions section, specify the date and time when you want to start synchronizing user data between Avaya Aura® Device Services and the LDAP server.
4. Select the **Repeat** check box and specify a period between consecutive synchronization attempts.
5. **(Optional)** To immediately synchronize the user data, click **Force LDAP Sync**.
Immediate synchronization does not affect scheduled synchronizations.
6. Click **Save**.

Related links

[Enabling automatic registration for an LDAP group](#) on page 170

[Synchronization with the LDAP server fails](#) on page 409

Stopping synchronization with the LDAP server

About this task

You can stop a running synchronization gracefully if the synchronization is stuck in the "In Progress" state.

Stopping a running synchronization does not affect scheduled synchronizations.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
2. In the User Synchronization Update Instructions area, click **Stop**.

The synchronization status changes to "Stopped".

LDAP user deletion confirmation

Avaya Aura® Device Services periodically synchronizes user data with enterprise LDAP servers to keep the internal user database up-to-date. If a user is deleted or marked as inactive in LDAP, Avaya Aura® Device Services deletes this user from the internal database. Therefore, the user will be deleted from all services that use this database, such as Avaya Spaces or Automatic Configuration.

There might be use cases when LDAP indicates that a user is deleted or marked as inactive, although the user remains in LDAP. For example, this might happen if the email attribute is not mapped correctly to a user in LDAP or if an invalid search filter is configured on an LDAP server. Consequently, the user deletion from the Avaya Aura® Device Services database might cause a service disruption for the user.

Avaya Aura® Device Services can track the number of users deleted or marked as inactive in LDAP between two consecutive synchronization events. Many deleted or marked inactive users might indicate that LDAP provides incorrect status for some of these users to Avaya Aura® Device Services. Therefore, user deletion from the internal database might not be required. You can configure Avaya Aura® Device Services not to automatically delete from the internal database users deleted from LDAP if the number of deleted users exceeds a certain threshold. If Avaya Aura® Device Services detects that the number of users deleted from LDAP since the last synchronization exceeds the specified threshold, Avaya Aura® Device Services does the following:

- Displays a warning on the Enterprise Directory page of the web administration portal prompting you to confirm the user deletion.
- Raises an alarm on System Manager or on other SNMP server configured in your deployment.

You must manually confirm or abort the user deletion from the internal Avaya Aura® Device Services database. Avaya Aura® Device Services keeps the users pending deletion in the database until you explicitly confirm the deletion.

If the number of users deleted or marked as inactive in LDAP since the last synchronization event does not exceed the threshold, Avaya Aura® Device Services deletes these users from the internal database automatically.

Note:

- Operations on the internal database do not affect LDAP user data. For example, if you decide to keep a user deleted from LDAP in the internal database, this user is not restored on LDAP. This user will exist in the internal Avaya Aura® Device Services database only.
- If you do not use automatic synchronization with LDAP servers, Avaya Aura® Device Services tracks the number of users deleted from LDAP since the last forced synchronization.

LDAP user deletion alarm

If the number of users deleted from LDAP since the last synchronization exceeds the specified threshold, Avaya Aura® Device Services raises an alarm on System Manager or on other SNMP server configured in your deployment. This alarm is cleared in the following instances:

- You manually confirm the user deletion before the next synchronization.
- You disable the **When Hard/Soft delete warning** check box on the Enterprise Directory page.
- The number of users deleted from LDAP before the next synchronization does not exceed the threshold.

Enabling the LDAP user deletion policy

About this task

You can configure Avaya Aura® Device Services to keep users deleted from LDAP in the internal database if the number of users deleted from LDAP since the last synchronization event exceeds a certain threshold. Avaya Aura® Device Services does not automatically delete these users from the internal database and prompts you to confirm or abort the user deletion.

The user deletion warning applies to all LDAP servers in your deployment. You cannot enable the warning for a specific LDAP server. The threshold value is the same for all LDAP servers in your deployment. However, the number of deleted users is tracked separately for each LDAP server.

The default threshold value is 50 users.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
2. In the Hard/Soft Delete User Warning section, select the **Enable Hard/Soft Delete warning** check box.
3. In the text box, specify an appropriate user deletion threshold.
The range is 1 to 100000.
4. Click **Save**.

Avaya Aura® Device Services starts tracking the number of users deleted from LDAP servers since the previous synchronization event.

Managing LDAP users pending deletion

About this task

If the number of users deleted from an LDAP server since the previous synchronization event exceeds the specified threshold, Avaya Aura® Device Services does not delete these users from the internal database automatically. You must confirm the user deletion manually.

Before you begin

Enable the LDAP user deletion warning.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
2. In the Hard/Soft Delete user warning section, navigate to the table with LDAP servers.
3. To view the detailed information about the users pending deletion, click **View details** for an appropriate LDAP server.
4. To confirm the user deletion from an LDAP server, select the **Allow to delete in next sync** check box for the LDAP server.
5. Click **Save**.

Disabling the LDAP user deletion policy

About this task

If you disable the LDAP user deletion policy, Avaya Aura® Device Services will always automatically delete from the internal database all users that are considered as deleted from LDAP.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
2. In the Hard/Soft Delete User Warning section, clear the **Enable Hard/Soft Delete warning** check box.
3. 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), and which language is 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 configuring 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**.
Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.
2. Configure the language setting:

Parameter	Description	Default value
Language used in Directory	The language code of one of the languages supported by Avaya Aura® Device Services.	English (en)

- Click **Save**.
- Click **Modify Attribute Mappings**.
- Configure the following settings:

Parameter	Description	Default value
NativeFirstName	The attribute that stores the “given name” of the user in the language of the LDAP server.	givenName
NativeSurName	The attribute that stores the “surname” of the user in the language of the LDAP server.	sn
GivenName	This is only applicable if the language in AD is one of the non-Latin script based ones.	
SurName	This is only applicable if the language in AD is one of the non-Latin script based ones.	

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](#).

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.

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

Adding a trusted host

Procedure

- On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > Trusted Hosts**.
- Click **Add**.
- 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 the Avaya Aura® Device Services CLI as an administrator.
2. Run the `cdto 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 johndoe@domain.com.`

For more information about this command, see [runUserDiagnostics tool](#) on page 462.

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 Avaya Workplace 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 209.

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 211.

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 following is an example of a CSV file used to uploading user data to Open LDAP:

```
Given Name,Last Name,Email Address,Phone Number,Image,Department
Aiden,Johnson,aiden_johnson@company.com,123456789,Images/aiden_johnson.jpg,Sales
James,Edwards,james_edwards@company.com,123450001,,Support
Harry,Anderson,harry_anderson@company.com,123451111,Images/harry_anderson.jpg,Support
```

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

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:

Attribute	Description	Is required	Example
Given Name	First name of the user.	Yes	Aiden
Last Name	Last name of the user.	Yes	Johnson
Email Address	Email address of the user.	Yes	aiden_johnson@company.com
Phone Number	Phone number of the user.	Yes	123456789
Image	Relative path to the user photo in the image folder.	No	Images/aiden_johnson.jpg
Department	Department of the user.	No	Sales

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:
James,Edwards,james_edwards@company.com,123450001,,Sales.

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`.

Optional structure of a CSV file if using Microsoft Excel

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:

	A	B	C	D	E	F
1	Given Name	Last Name	Email Address	Phone Number	Image	Department
2	Aiden	Johnson	aiden_johnson@company.com	123456789	Images/aiden_johnson.jpg	Sales
3	James	Edwards	james_edwards@company.com	123450001		Support

	A	B	C	D	E	F
4	Harry	Anderson	harry_anderson@company.com	123451111	Images/harry_anderson.jpg	Support

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 211.

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. In Server Address and Credentials area, click **Modify Attribute Mappings**.
5. For the PictureURL attribute, enter `jpegPhoto` in the **Custom Field Name** field.
6. Click **Save**.
7. To apply the changes immediately, click **Force LDAP Sync** on the Enterprise Directory page.

Configuration of LDAP contact search

You can use Avaya Aura[®] Device Services to configure contact search rules in LDAP directories for Avaya Workplace Client. You can do the following:

- If you have multiple LDAP directories in your deployment, select which LDAP directories are used for the contact search.
- Specify which additional base context DNs to use for the contact search.
- Limit the contact search scope to the group or department of a user that performs the search operation.

These search rules apply both to Avaya Workplace Client normal search and to quick search.

Avaya Aura[®] Device Services uses the Organizational Unit (OU) attribute to determine whether the user belongs to a group or department.

The impact of the contact search scope on the contact search on System Manager

In an Avaya Aura[®] environment, Avaya Aura[®] Device Services performs the contact search on System Manager differently depending on whether the search scope is limited to a user's own group or department.

Note:

In an environment without Avaya Aura[®], Avaya Aura[®] Device Services does not perform the contact search on System Manager.

When the search is performed in all groups or departments, Avaya Aura[®] Device Services performs the search in parallel both in LDAP directories and on System Manager. Avaya Aura[®] Device Services then displays all the results that match the search criteria.

When the search scope is limited to the user's own group or department, Avaya Aura[®] Device Services performs the search in LDAP directories first and then on System Manager as follows:

1. Avaya Aura[®] Device Services searches for contacts that match the search criteria in the LDAP directories and then displays found contacts.
2. After the search in the LDAP directories completes, Avaya Aura[®] Device Services retrieves email addresses of the found contacts.
3. Avaya Aura[®] Device Services searches for contacts on System Manager using these email addresses as a search criteria and then displays found contacts.

For example, an LDAP directory contains a contact with the "UserName" name and the "address@example.com" email address. System Manager contains a contact with the same

name, whose email address is “anotherAddress@example.com”. If a client searches for “UserName”, Avaya Aura® Device Services finds a user with this name in LDAP and then uses the user's email address, “address@example.com”, to search for contacts on System Manager. Since System Manager does not contain a user with the “address@example.com” email address, Avaya Aura® Device Services only displays the contact found in the LDAP directory in the search results.

Selecting LDAP servers for the contact search

About this task

Use this procedure to select LDAP directories that Avaya Aura® Device Services uses for the contact search. Avaya Aura® Device Services performs the search only in those LDAP directories that are enabled for the contact search.

By default, the starting location for the contact search is specified in the Base Context DN parameter of a LDAP directory.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
2. Select the appropriate LDAP server.
3. Do one of the following:
 - To use the LDAP server for contact search, select the **Use for contact search** check box.
 - To ignore the LDAP server for contact search, clear the **Use for contact search** check box.
4. Repeat steps 2 to 3 for all other LDAP servers configured on your Avaya Aura® Device Services.
5. Click **Save**.

Next steps

- If required, specify additional search locations within LDAP directories as described in [Setting up contact search for additional base context DNs](#) on page 213.
- Configure the contact search scope as appropriate. For more information, see [Limiting the contact search scope to user's own group or department](#) on page 214.

Setting up contact search for additional base context DNs

About this task

You can use additional base context DNs to specify multiple search locations within the same LDAP directory. Use this procedure to select which of these additional base context DNs Avaya Aura® Device Services uses for the contact search.

Before you begin

Configure additional base context DNs as described in [Configuring additional base context DNs](#) on page 193.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
2. Select the appropriate LDAP server.
3. Click **View/Edit** located next to the **Use additional Base Context DN** check box.
Avaya Aura® Device Services displays the list of additional base context DN's configured for the LDAP directory.
4. For each additional base context DN, do the following:
 - To use the additional context DN for contact search, select the **Use for contact search** check box for this DN.
 - To ignore the additional context DN for contact search, clear the **Use for contact search** check box for this DN.
5. Click **Save**.
6. Repeat steps 2 to 5 for other LDAP directories that you use for contact search.
7. In the Server Address and Credentials section, click **Save**.

Next steps

Configure the contact search scope as appropriate. For more information, see [Limiting the contact search scope to user's own group or department](#) on page 214.

Limiting the contact search scope to user's own group or department

About this task

By default, Avaya Aura® Device Services searches for contacts in all groups and departments of all LDAP directories selected for contact search. You can limit the search scope so that the user can only search for contacts that belong to the user's own group or department.

When enabled, this limitation applies to all LDAP directories in your deployment. The configured search rules apply to both Avaya Workplace Client normal search and quick search functionality.

Note:

When you change the contact search scope, the changes are immediately applied to the normal search only. For the quick search, a client continues to use the previously configured search scope until the user re-logs in to the client.

Before you begin

Select LDAP servers you want to use for contact search as described in [Selecting LDAP servers for the contact search](#) on page 213. Avaya Aura® Device Services searches for contacts only in the LDAP directories that you selected for contact search.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **System Parameters > Parameter Configuration**.
2. For the **RESTRICTED_CONTACT_SEARCH** parameter, select the appropriate value as follows:
 - **true**: To exclude contacts that are not a part of the user's own group or department when the user searches for contacts.
 - **false**: To include contacts from all groups or departments of all LDAP directories enabled for contact search, when a user searches for contacts.
3. Click **Save**.

Limiting the System Manager contact search

Before you begin

Select LDAP servers you want to use for contact search as described in [Selecting LDAP servers for the contact search](#) on page 213. Avaya Aura® Device Services searches for contacts only in the LDAP directories that you selected for contact search.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **System Parameters > Parameter Configuration**.
2. For the **RESTRICTED_SMGR_CONTACT_SEARCH** parameter, select the appropriate value as follows:
 - **true**: To exclude System Manager contacts from the search results when a user searches for contacts.
 - **false**: To include System Manager contacts in the search results when a user searches for contacts. This option is the default value.
3. Click **Save**.

Disabling contact search for a LDAP server

About this task

Use this procedure to disable the contact search functionality for a LDAP server.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise Directory**.
2. Select the LDAP server for which you want to disable the contact search functionality.
3. Clear the **Use for contact search** check box.
4. Click **Save**.

5. Log in to the Avaya Aura® Device Services CLI as an administrator.
6. Run the following commands:

```
cdto misc  
sudo ./clearPhoneNumberLastSynch.sh
```

7. To apply the changes immediately, on the web administration portal, click **Force LDAP Sync** on the Enterprise Directory page.

Chapter 7: Avaya Aura® Device Services network settings configuration

Starting from Release 8.1.5, you can modify the network settings of an Avaya Aura® Device Services node from a single location by running the `cliChangeNet.sh` script from the node CLI. You can configure the following settings:

- IP address of the node
- Subnet mask
- Host name of the node
- Domain name of the node
- Default gateway IP address
- DNS server IP address
- Default search list
- NTP server IP or FQDN
- Time zone
- Country

The following are examples of scenarios where you can use the `cliChangeNet.sh` script:

- Re-configuring network settings for your entire Avaya Aura® deployment.
- Re-configuring network settings for your Avaya Aura® Device Services standalone system or cluster.
- Updating network configuration for an Avaya Aura® Device Services node. For example, when moving one or several Avaya Aura® Device Services nodes to another data center.

Changing your DNS or NTP servers.

cliChangeNet.sh script limitations

- You cannot use the `cliChangeNet.sh` script in AWS OVA-based deployments.
- You cannot use the `cliChangeNet.sh` script to change the following Avaya Aura® Device Services network settings:
 - Front-end FQDN
 - Virtual IP address
 - Utility Server virtual IP address

- Utility Server FQDN

In an Avaya Aura® environment, you also cannot use `cliChangeNet.sh` to update the following settings:

- System Manager FQDN
- Session Manager Management IP address
- Session Manager Asset IP address

To update these settings, use the Avaya Aura® Device Services configuration utility.

- In a cluster deployment, if you use optional Avaya Aura® Device Services features, such as OAuth, Utility Server, or onboard Open LDAP, you might need to perform additional configuration steps using the configuration utility.
- If you change the IP addresses or FQDN of an Avaya Aura® Device Services node, you *cannot* restore the data using backups created before you made these network changes. This limitation applies to manual and automatic backups.
- If you perform a rollback after changing Avaya Aura® Device Services IP addresses or FQDNs, Avaya Aura® Device Services continues to use these new IP addresses or FQDNs after the rollback. The rollback process does not revert IP addresses or FQDN changes.

Avaya Aura® Device Services network configuration checklist

Perform the following tasks to configure Avaya Aura® Device Services network settings:

No.	Task	Description	✓
1	Prepare your virtual machines for configuring network settings. Back up Avaya Aura® Device Services.	See Prerequisites for configuring Avaya Aura Device Services network settings on page 219.	
2	Configure network settings using the <code>cliChangeNet.sh</code> script.	See Configuring network settings using the cliChangeNet.sh script on page 220. In a cluster environment, perform this procedure on the seed node first and then on all non-seed nodes.	
3	Configure network settings using the Avaya Aura® Device Services configuration utility.	You can configure certain Avaya Aura® Device Services network settings only using the configuration utility. You must also use the configuration utility to finalize the configuration process if you change certain network settings using the <code>cliChangeNet.sh</code> script. For more information, see Configuring network settings using the Avaya Aura Device Services configuration utility on page 221.	

Prerequisites for configuring Avaya Aura® Device Services network settings

There are several prerequisites for configuring Avaya Aura® Device Services network settings. These prerequisites are not required if you only need to update the DNS or NTP server IP addresses.

The following prerequisites are applicable both for Avaya Aura® environments and for environments without Avaya Aura®:

- If you plan to change IP addresses or FQDNs of Avaya Aura® Device Services nodes and you use third-party CA identity certificates, obtain new certificates with appropriate FQDNs from your CA.

 Note:

In an environment without Avaya Aura®, Avaya Aura® Device Services always uses third-party CA identity certificates. Therefore, you must always update identity certificates when you change IP address or FQDNs of Avaya Aura® Device Services.

- If you plan to change the IP address of an Avaya Aura® Device Services node, ensure that the new IP addresses are available in the appropriate subnet.
- If you plan to change the IP address of an Avaya Aura® Device Services node, ensure that the network adapter or virtual switch of the Avaya Aura® Device Services virtual machine is configured with the appropriate subnet for this IP address.
- In a cluster deployment, If you plan to change FQDNs of Avaya Aura® Device Services nodes and if you use onboard Open LDAP, back up user data stored on Open LDAP using the following command:

```
tar -zcf /tmp/<BACKUP_NAME>.tar.gz /media/data/ldap/*
```

For example:

```
tar -zcf /tmp/ldapDBBKUP.tar.gz /media/data/ldap/*
```

 Important:

When you re-enable Open LDAP replication after applying network changes, all Open LDAP user data is erased as part of the process. Therefore, to keep Open LDAP user data, you must back up user data and restore it after completing network configuration.

The following prerequisites are applicable for Avaya Aura® environments only:

- If you plan to change network settings of System Manager or Session Manager in your deployment, complete these changes before updating any network settings on Avaya Aura® Device Services.
- If you plan to change the IP address or FQDN of an Avaya Aura® Device Services node, add a new element for this node on System Manager on the **Services > Inventory > Manage Elements** page.

 Note:

If you change the Session Manager IP address or FQDN, you must also create a new Session Manager element on System Manager before starting to configure Avaya Aura® Device Services network settings.

- If you plan to change IP addresses or FQDNs of Avaya Aura® Device Services nodes and you do not use DNS servers in your deployment, do the following:
 - Add host names of all Avaya Aura® Device Services nodes to the `/etc/hosts/` file on System Manager.
 - Add the System Manager host name to `/etc/hosts/` files on all Avaya Aura® Device Services nodes.

There are no specific prerequisites for environments without Avaya Aura®.

Configuring network settings using the `cliChangeNet.sh` script

About this task

Use this procedure to configure network settings of an Avaya Aura® Device Services node.

This procedure applies to OVA-based and software-only deployment types.

 Important:

- You cannot use the `cliChangeNet.sh` script in AWS OVA-based deployments.
- Avaya Aura® Device Services is unavailable when applying new network settings.

In a cluster deployment, perform this procedure on each cluster node starting from the seed node.

Before you begin

Review and complete prerequisites listed in [Prerequisites for configuring Avaya Aura Device Services network settings](#) on page 219.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command to navigate to the script location:

```
cdto misc
```
3. Run the following command:

```
sudo ./cliChangeNet.sh
```
4. Configure network settings as appropriate:
 - To change the existing value, enter a new value and press `Enter`.
 - To keep the existing value, do not enter anything and press `Enter`.

5. When prompted to apply the changes, do one of the following:
 - To confirm the changes, enter `Y`.
 - To discard any changes you made in the network configuration, enter `N`.
6. After the configuration process is complete, run the following command to restart Avaya Aura® Device Services:


```
svc aads restart
```
7. In a cluster deployment, repeat the previous steps on all remaining nodes.

Next steps

Complete network configuration as described in [Configuring network settings using the Avaya Aura Device Services configuration utility](#) on page 221.

Configuring network settings using the Avaya Aura® Device Services configuration utility

About this task

You must use the Avaya Aura® Device Services configuration utility to configure the following network settings:

- Front-end FQDN
- Virtual IP address
- Utility Server virtual IP address and FQDN
- System Manager FQDN
- System Manager IP addresses

You might also need to perform additional actions to complete the configuration process after configuring Avaya Aura® Device Services network settings using the `cliChangeNet.sh` script. The exact actions that you must perform depend on the following:

- Whether you modified IP addresses of System Manager and Session Manager.
- Whether you have a standalone or cluster deployment.
- Whether you use optional Avaya Aura® Device Services features, such as OAuth, Utility Server, or onboard Open LDAP.

You do not need to perform this procedure if you only change DNS or NTP server IP addresses.

Before you begin

- Configure network settings as described in [Configuring network settings using the cliChangeNet.sh script](#) on page 220. In a cluster deployment, configure network settings on each cluster node.
- In a cluster deployment, if you use onboard Open LDAP, back up user data stored on Open LDAP.

 Important:

When you re-enable Open LDAP replication after applying network changes, all Open LDAP user data is erased. Therefore, you must back up user data and then re-upload user data using the Avaya Aura® Device Services web portal after completing network configuration.

Procedure

1. Log in to the Avaya Aura® Device Services as an administrator.
2. Run the following command to start the configuration utility:

```
app configure
```

3. Do the following to update front-end FQDN settings:
 - a. Navigate to **Front-end host, System Manager and Certificate Configuration settings**.
 - b. If you updated the front-end FQDN of the virtual IP address, in **Front-end FQDN**, type the new FQDN.
 - c. If you updated the local FQDN of the node, in **Local frontend host**, type the new FQDN of the node.
 - d. In **Keystore password**, type the Keystore password you used when installing Avaya Aura® Device Services.
 - e. Click **OK** and then click **Apply**.
4. If you updated the virtual IP address of Avaya Aura® Device Services, do the following:
 - a. Navigate to **Clustering Configuration > Virtual IP Configuration** menu.
 - b. In **Virtual IP address**, type the new virtual IPv4 address.
 - c. If you use IPv6, in **Virtual IPv6 address**, type the new virtual IPv6 address.
 - d. Click **OK** and click **Apply**.

 Note:

Perform this step on the seed and backup nodes only. Do not perform this step on other non-seed nodes.

5. In an Avaya Aura® environment, if you need to update System Manager settings, do the following:
 - a. Navigate to **Front-end host, System Manager and Certificate Configuration settings**.
 - b. In **System Manager FQDN**, type the System Manager FQDN.
 - c. In **System Manager Enrollment Password**, type the enrollment password of the System Manager.
 - d. In **Keystore password**, type the Keystore password you used when installing Avaya Aura® Device Services.

- e. Click **OK** and then click **Apply**.
6. If you need to update third-party identity certificates, import certificates with appropriate FQDNs to Avaya Aura® Device Services as described in [Importing third-party CA-signed certificates](#) on page 236.
- * **Note:**
 - You must update identity certificates if you change IP addresses or FQDNs of any of Avaya Aura® Device Services nodes.
 - In an environment without Avaya Aura®, Avaya Aura® Device Services always uses third-party identity certificates.
 - If you use System Manager certificates, these certificates are automatically re-generated when you perform step 5.
7. In an Avaya Aura® environment, if you need to update Session Manager IP addresses, do the following:
 - a. Navigate to the **Session Manager Configuration** menu.
 - b. In **Session Manager Management IP**, type the new Session Manager Management IP address.
 - c. In **Session Manager Asset IP**, type the new Session Manager Asset IP address.
 - d. Select **Apply**.
8. To update the Utility Server virtual IP address and FQDN, do the following:
 - a. Navigate to the **Utility Server configuration** menu.
 - b. In **Utility Server VIP**, type the new virtual IPv4 address of the Utility Server.
 - c. If you use IPv6, in **Utility Server Ipv6**, type the new virtual IPv6 address of the Utility Server.
 - d. In **Utility Server FQDN**, type the new FQDN of the Utility Server.
9. In **Main Menu**, click **Continue** and click **Yes**.
10. When the configuration process completes, click **Continue**.
11. In a cluster deployment, perform steps 2 to 3 and then steps 5 to 10 on all remaining nodes of the cluster.
You must perform step 4 on the seed node only.
12. In a cluster deployment, on each cluster node, run the `app listnodes` command and ensure that all cluster nodes have the “live” status.
13. In a cluster deployment, configure RSA public and private keys for internode SSH communication as described in [Configuring RSA public and private keys for SSH connections in a cluster](#) on page 387.
14. In a cluster deployment, if SSO/OAuth is enabled on Avaya Aura® Device Services, re-configure OAuth replication on all nodes in the cluster.

For information about configuring OAuth replication, see [Enabling OAuth database replication in a cluster environment](#) on page 151.

15. In a cluster deployment, if you use onboard Open LDAP, do the following:

a. On each cluster node, run the following commands:

```
cdto openldap
sudo ./recover_openldap.sh
```

b. On each cluster node, enable Open LDAP replication as described in [Enabling Open LDAP replication](#) on page 391.

c. On the seed node, run the following command to restore Open LDAP user data from a backup:

```
tar -xzf /tmp/<BACKUP_NAME> -C /
```

For example:

```
tar -xzf /tmp/ldapDBBKUP.tar.gz -C /
```

Next steps

If you have components in your deployment that use Avaya Aura® Device Services FQDNs or IP addresses, update these settings accordingly. For example, the following components can use Avaya Aura® Device Services FQDNs or IP addresses:

- Avaya Aura® Web Gateway uses Avaya Aura® Device Services FQDN if OAuth is configured. System Manager uses Avaya Aura® Device Services FQDNs on the Elements page.
- External load balancer uses Avaya Aura® Device Services FQDN in its certificate.

Chapter 8: Certificate management

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.

Generating System Manager identity certificates

About this task

Use this procedure to generate System Manager security identity certificates.

Avaya Aura® Device Services does not accept a generated System Manager certificate if:

- The certificate contains an unsupported critical extension.
- The certificate expired.
- The start date of the certificate is in the future.

Avaya Aura® Device Services displays a warning message if the generated certificate cannot be imported. To fix the issue, contact the System Manager administrator.

This procedure is not applicable if you use Avaya Aura® Device Services in an environment without Avaya Aura®.

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.

Related links

[Managing CSRs](#) on page 227

[Managing keystore data](#) on page 230

[Configuring expiration notifications for identity certificates](#) on page 231

[Managing server interface certificates](#) on page 232

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 227.
- 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 229.

Related links

[Managing identity certificates](#) on page 226

[Creating CSRs](#) on page 227

[Processing CA signing requests](#) on page 229

[Managing server interface certificates](#) on page 232

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 229.

Note:

For Open LDAP, the **Subject Alternative Name** section must contain the `localhost.localdomain` and, for IPv6, `localhost6.localdomain` records.

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 229.

Related links

[Managing CSRs](#) on page 227

[Creating a CSR for a certificate to connect Avaya Aura Device Services to the Avaya Aura Web Gateway](#) on page 228

[Create Certificate Signing Request screen field descriptions](#) on page 229

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

1. Log in to the Avaya Aura® Device Services web administration portal with the Security administrator role.
2. Navigate to **Security Settings > Certificate Management > Identity Certificates**.
3. In the Certificate Signing Requests area, click **Create**.
4. In the Create Certificate Signing Request window, click **Show Advanced Settings**.
5. Select **Specify SAN Manually**.
6. 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 229.
2. Assign the signed certificate to the Internal server interface as described in [Managing server interface certificates](#) on page 232.

Related links

[Creating CSRs](#) on page 227

Create Certificate Signing Request screen field descriptions

Name	Description
Alias	The name of the certificate
Common Name	The FQDN of the node. For example, <code>amm.example.com</code> You cannot provide wildcard (*) characters in this field.
Use Existing FQDNs for SAN	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.
Specify SAN manually	Use this option to manually specify additional FQDNs or IP addresses for which the certificate should be generated.
Subject Alternative Name	An optional text field that can be used to further identify this certificate. You can provide multiple entries in this field. You cannot provide wildcard (*) characters in this field.
Key Bit Length	The certificate key length in bits.
Signature Algorithm	The hash algorithms to be used with the RSA signature algorithm.
Organizational Unit	The group within the company or organization creating the certificate.
Organization	The name of the company or organization creating the certificate.
City/Locality Name	The city where the certificate is being created.
State/Province Name	The state/province where the certificate is being created.
Country (ISO 3166)	The name of the country within which the certificate is being created in the ISO 3166 format. For more information about the format, see ISO 3166 country codes .

Related links

[Creating CSRs](#) on page 227

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.

Related links

[Managing CSRs](#) on page 227

Managing keystore data

Procedure

In the Keystore area, do one of the following:

- To import keystore data, click **Import** and then import keystore data.

For more information, see [Importing keystore data](#) on page 230.

- 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 keystore file details, click **Details**.
- To remove an existing keystore file, select it and then click **Delete**.

Related links

[Managing identity certificates](#) on page 226

[Importing keystore data](#) on page 230

Importing keystore data

About this task

Use this procedure to import third-party identity certificates to the Avaya Aura® Device Services Keystore.

You cannot import a certificate if:

- The certificate contains an unsupported critical extension.
- The certificate expired.
- The start date of the certificate is in the future.

Avaya Aura® Device Services displays a warning message if a certificate cannot be imported.

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.

Related links

[Managing keystore data](#) on page 230

Configuring expiration notifications for identity certificates

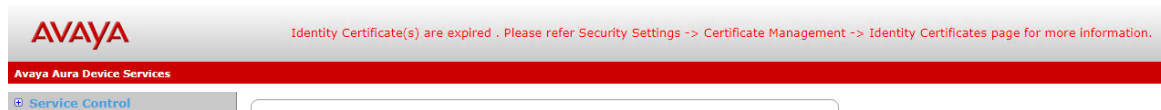
About this task

If an identity certificate expires, Avaya Aura® Device Services can no longer provide secure connections with browser clients. You can specify a number of days before the certificate expiry date when Avaya Aura® Device Services starts to generate certificate expiration notifications.

Avaya Aura® Device Services generates the following certificate expiration notifications:

- A warning message on the Avaya Aura® Device Services web administration portal.

The following image shows a warning message example:



- An alarm on System Manager or on other SNMP server configured in your deployment.

If a certificate expires, Avaya Aura® Device Services clears this alarm and generates the "certificate expired" alarm. After you renew the certificate, Avaya Aura® Device Services clears all certificate expiration alarms.

- A log entry in the `AADS_alarm.log` file.

* Note:

For the detailed information about the certificate, see `AADS_audit.log`.

You *cannot* disable certificate expiration notifications.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Security Settings > Certificate Expiration**.
2. In **Start to send certificate about to expire notification**, type the required number of days before the certificate expiry date when you want to start receiving notifications.

The minimum value for this setting is one day. The maximum value for this setting is 366 days.
3. Click **Save**.

Related links

[Managing identity certificates](#) on page 226

Managing server interface certificates

About this task

Use this procedure to manage Keystore identity 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 232.

You cannot assign a certificate to an interface if:

- The certificate contains an unsupported critical extension.
- The certificate expired.
- The start date of the certificate is in the future.

Avaya Aura® Device Services displays a warning message if a certificate cannot be assigned to an interface.

If you assign a certificate only to a selected node, then you must restart the services on that node to apply the changes. If you assign a certificate to the entire cluster, 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**.

Related links

[Managing identity certificates](#) on page 226

[Certificate assignment descriptions](#) on page 232

Certificate assignment descriptions

Name	Description
Application	Specifies the interface for REST API to the clients.
Internal	Specifies the interface being used for server-to-server component communication.
OAM	Specifies the Operations, Administration, and Maintenance (OAM) interface.

Related links

[Managing server interface certificates](#) on page 232

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.
You cannot import a certificate if it contains unsupported critical extensions, expired, or if the start date of the certificate is in the future. If a certificate cannot be imported, Avaya Aura® Device Services displays a warning message.
 - **Details:** To view information about the certificate.
 - **Delete:** To delete the certificate from the truststore.
 - **Export:** To export the certificate in the PEM format.
 - **Propagate:** To propagate the certificate to all cluster nodes.
3. Restart Avaya Aura® Device Services after importing or deleting certificates for changes to take effect. For the cluster environment, restart all the nodes in the cluster for changes to take effect.

Certificate revocation management

Avaya Aura® Device Services can use TLS to communicate with the following deployment components securely:

- LDAP server
- System Manager
- Session Manager
- iView
- Avaya Spaces

To establish a secure TLS connection, Avaya Aura® Device Services uses digital identity certificates issued by a trusted Certificate Authority (CA). Before establishing a secure connection, Avaya Aura® Device Services verifies that the respective digital certificate is valid and not expired.

Sometimes, CA might revoke a certificate before it expires. For example, if the certificate public key is compromised. If you continue to use a revoked certificate, your TLS connection might be not secure and can be exploited by a malicious actor. To indicate that a certificate was revoked and should no longer be used, CA places this certificate in a Certificate Revocation List (CRL). This list is publicly available through a CRL distribution point URL. CRLs contain various information about revoked certificates, such as the certificate serial number and revocation date

and time. Avaya Aura® Device Services automatically downloads CRLs for all CAs that issued certificates used in your deployment to establish secure connections.

Avaya Aura® Device Services uses this data to determine whether a certificate can be used to establish a secure connection with a deployment component. Avaya Aura® Device Services fetches CRLs from CAs once every 24 hours.

Avaya Aura® Device Services writes events related to certificate revocation checks to the `AADS_audit.log` file.

 Note:

Avaya Aura® Device Services does not support certificate revocation checks using the Online Certificate Status Protocol (OCSP).

Revocation status

You can review the revocation status for each deployment component on the **Security Settings > Certificate Revocation** page in the Certificate Revocation Status table.

- **OK.** The Certificate is valid.
- **REVOKED.** The certificate is found in the CRL. An alarm is raised.
- **NETWORK_ERROR.** The CRL distribution point URL is not reachable. An alarm is raised.
- **FAILED_TO_VERIFY.** Not able to verify the CRL due to server-related issues.

If a certificate for a component is revoked, Avaya Aura® Device Services needs a new valid certificate from the Administrator of this component to replace the revoked certificate. As Administrator, you do need to perform any actions in Avaya Aura® Device Services. However, Avaya Aura® Device Services cannot establish connection with that particular component till the component certificate is replaced with a valid certificate.

Revocation validation

You can choose whether Avaya Aura® Device Services validates certificates.

NONE: Avaya Aura® Device Services does not check the certificate status before establishing the secure connection.

BEST_EFFORT: Avaya Aura® Device Services checks the certificate revocation status. Avaya Aura® Device Services considers a certificate *valid* if:

- The certificate is not in the CRL of the respective CA.
- The certificate revocation check returns a valid status, such as “good”, “verified”, or “unrevoked”, for the certificate.
- The CRL distribution point is not reachable due to network issues.

MANDATORY: Avaya Aura® Device Services checks the certificate status. Avaya Aura® Device Services considers a certificate valid *only* if the CRL of the respective CA does not contain this certificate. If Avaya Aura® Device Services cannot check the certificate status, the certificate is considered invalid.

Related links

[Cannot connect to System Manager after replacing a revoked System Manager certificate with a valid certificate](#) on page 404

Configuring the revocation check policy

About this task

You can configure a certificate revocation check policy on Avaya Aura® Device Services. When a revocation check policy is enabled, Avaya Aura® Device Services checks the revocation status of a certificate before establishing a secure connection using this certificate. If the certificate revocation status does not comply with the configured policy, the connection is refused.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Security Settings > Certificate Revocation**.
2. From **Certificate Revocation Validation**, select whether to use revoked certificates as follows:
 - **NONE**
 - **BEST_EFFORT**
 - **MANDATORY**
3. From **Check method**, select whether Avaya Aura® Device Services checks the revocation status of other certificates in a certificate chain:
 - **ONLY_END_ENTITY**: Avaya Aura® Device Services checks only the end-entity certificate in the certificate chain.
 - **CERTIFICATE_CHAIN**: Avaya Aura® Device Services checks the revocation status of all certificates in the certificate chain.
4. Click **Save**.

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.

You cannot import an LDAP certificate if:

- The certificate contains an unsupported critical extension.
- The certificate expired.
- The start date of the certificate is in the future.

Avaya Aura® Device Services displays a warning message if a certificate cannot be imported.

Before you begin

- Download the CA certificate chain for the CA that signed the LDAP server identity certificate in PEM format.
- If you want to use LDAP discovery using DNS SRV records, ensure that the Subject Alternative Name of the LDAP certificate contains FQDNs of all LDAP server instances that must be discoverable.

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 computer.
5. Click **Save**.

Avaya Aura® Device Services uploads the certificate to a secure LDAP Server. If a certificate is already uploaded, Avaya Aura® Device Services overwrites the existing certificate.

Importing third-party CA-signed certificates

About this task

If you do not use Avaya Aura® System Manager for certificate management, Avaya Aura® Device Services enables you to use certificates specific to your organization and have the certificates signed by a local or public certificate authority (CA).

The following procedure describes how to import third-party certificate files and corresponding key files using the configuration utility.

Before you begin

Import third-party root and all intermediate CAs into the following trust stores in order:

- The trust stores of each server that interacts with Avaya Aura® Device Services in your deployment, including System Manager, Session Manager, Avaya Aura® Session Border Controller, and Avaya Meetings Management servers.
- The Avaya Aura® Device Services trust store. This is required for intra-cluster communications where the Avaya Aura® Device Services identity certificate is presented to other servers within the cluster.

! Important:

You must perform the importing in order. Otherwise, a loss of service can occur because Avaya Aura® Device Services cannot communicate with some or all of the mentioned servers.

Procedure

1. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.
2. Select **Front-end host, System Manager and Certificate Configuration** and do one of the following:
 - If you use Avaya Aura® Device Services in an Avaya Aura® environment, continue from step 3.
 - If you use Avaya Aura® Device Services in an environment without Avaya Aura®, continue from step 6.
3. Configure the System Manager connection details:
 - **System Manager FQDN**
 - **System Manager HTTPS Port** or the **Front-end port for reverse proxy**, if applicable
To configure the reverse proxy port number, you must first set the **Override port for reverse proxy** setting to `y` (yes).
4. Configure the **System Manager Enrollment Password** option.
The System Manager enrollment password is used for adding the certificates to the trust store of the client applications.
5. Set **Use System Manager** to `n` (no).
The menu displays options for importing individual certificate files and the corresponding key files.
6. Configure the following options to provide the paths to the certificate and key files:
 - REST interface key file
 - REST interface certificate file
 - OAM interface key file
 - OAM interface certificate file
 - node key file
 - node certificate file
 - signing authority certificate file

The certificate and the corresponding key file must be present on the server when they are imported. If one pair of files is not imported because one or both files are missing, the other files may still be imported so that you can selectively replace individual certificates. To generate certificates, you can also use Avaya Aura® System Manager and replace individual certificates, such as the front-end certificates.

7. Configure the **Keystore password** option.

This password is used for adding the certificates to the trust store of the client applications. The role of the keystore password is similar to the role of the Avaya Aura® System Manager enrollment password in the configurations that use the Avaya Aura® System Manager root certificate.

8. Restart Avaya Aura® Device Services and check the configuration utility log files to ensure that the certificates were imported successfully.

Chapter 9: Web Deployment service management

The Web Deployment service enables appcast for Avaya Workplace Client desktop applications. 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. Avaya Aura® Device Services 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>`. In this URL, AADS_SERVER_ADDRESS is the Avaya Aura® Device Services front-end FQDN or virtual IP address.
- 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, Avaya Workplace Client will get the APPCAST_URL setting from the Dynamic Configuration service response for the Web Deployment service.

You must set the APPCAST_URL setting to `https://<AADS_SERVER_ADDRESS>:443/acs/resources/webdeployment`. In this URL, AADS_SERVER_ADDRESS is the Avaya Aura® Device Services front-end FQDN or virtual IP address.

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 Workplace Client for Windows to connect to the Web Deployment service](#) on page 389.

*** 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 Workplace Client for Windows, you can upload `.exe` or `.msi` installation files. For Avaya Workplace Client for Mac, you can upload update and installation `.dmg` files, which are packaged in a `.zip` archive.

For Avaya Workplace Client for Windows installer, you can select non-interactive upgrade mode. In non-interactive mode, the user does not interact with the installer after starting the upgrade process.

Procedure

1. Download Avaya Workplace Client for Mac or Avaya Workplace Client for Windows installation files from the Avaya Support website.

You must have PLDS access to download these files.

2. If you are uploading Avaya Workplace Client for Mac, pack both update and installation `.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.

By default, the update file has the `AvayaWorkplaceMacOS-<version>-Sparkle.dmg` file name and the installation file has the `AvayaWorkplaceMacOS-<version>.dmg` file name.

! Important:

If you change the default file names before uploading, ensure that the new file name of the update file contains the case-insensitive word “sparkle”. For example: `AEUpdSparkleLatest.dmg`. Otherwise, the upload process might not work as expected.

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**.

Avaya Aura® Device Services 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, Avaya Aura® Device Services automatically adds *Avaya Workplace* before the given title.

For example, if you type the update name: *Windows Version 2.0: Critical update*, Avaya Aura® Device Services displays: *Avaya Workplace 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 Workplace Client release.
8. In the **OS** field, select one of the following platforms for the Avaya Workplace Client release:

- windows
- macOS

 Note:

If you select macOS, the **ED Signature** field is enabled. The Administrator can add the ED signature for Mac OS binary upload.

9. **(Optional)** For Avaya Workplace Client for Windows, if you want to enable non-interactive upgrade for the client, in **Installer Arguments**, type `/passive AUTOSTARTONINSTALLCOMPLETE=1`.

Non-interactive upgrade requires no user interaction with the installer. After the user starts the upgrade process, the client installs updates automatically using the default options.

By default, the Web Deployment service upgrades Avaya Workplace Client for Windows in interactive mode.

10. Do one of the following:

- If you are uploading an Avaya Workplace Client 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 Workplace Client 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 Workplace Client for Windows client installer, leave the **Min OS version** field blank.

11. In **File**, click **Choose File** and select one of the following files to upload:

- For Avaya Workplace Client for Windows, select the `.exe` or `.msi` installation file.
- For Avaya Workplace Client for Mac, select the `.zip` archive containing the `.dmg` installation files.

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, Avaya Aura® Device Services auto populates the **Size (in bytes)** and the **MD5 Hash** field.

12. 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.

Avaya Aura® Device Services displays a pop up to specify the user credentials to upload the client installer and a confirmation dialog box to indicate the upload status.

13. 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.

14. Click **Save** to save the settings.

Avaya Aura® Device Services populates the data in the table at the bottom of the page. For more information about fields, see [Appcast items field descriptions](#) on page 242. 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 Workplace Client installers that you can download using the Web Deployment service.

Name	Description
Title	The name of the updates or appcast for the client installer.
Description	The description of the client installer updates or appcast.
Version	The version information for the Avaya Workplace Client release.
Publish Date	The date and time when the installer was uploaded onto the Web Deployment service.
OS	The platform of the Avaya Workplace Client installer. You can choose from one of the following options: • windows • macOS
Download URL	The URL that specifies the location of the Avaya Workplace Client installer.

Name	Description
Downloads	The number of times the appcast file has been downloaded using the download URL.
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**.

Avaya Aura® Device Services displays the Software Update Deployment page.

2. On the bottom of the Software Update Deployment page, double-click an entry in the table.

Avaya Aura® Device Services displays the Edit appcast item page.

3. Edit the settings that you want to change.

4. Click **Save**.

Avaya Aura® Device Services populates the updated data in the table at the bottom of the page.

Selecting interactive or non-interactive upgrade mode for Avaya Workplace Client for Windows

About this task

You can configure an Avaya Workplace Client for Windows installer to run in either interactive or non-interactive mode.

- Interactive upgrade is the default upgrade option that requires user interaction with the installer.
- Non-interactive upgrade requires no user interaction with the installer. After the user starts the upgrade process, the client installs updates automatically using the default options.

If you configured non-interactive upgrade for an installer, the user cannot run this installer in interactive mode.

The minimum supported Avaya Workplace Client for Windows version for this feature is 3.18.

Procedure

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

Avaya Aura® Device Services displays the Software Update Deployment page.

2. In the table, double-click the appcast entry that you want to modify.

Avaya Aura® Device Services displays the Edit appcast item page.

3. Do one of the following:

- To enable non-interactive upgrade, in the **Installer Arguments** field, type `/passive AUTOSTARTONINSTALLCOMPLETE=1`.
- To disable non-interactive upgrade and to enable interactive upgrade, remove the `/passive AUTOSTARTONINSTALLCOMPLETE=1` entry from the **Installer Arguments** field.

4. Click **Save**.

Avaya Aura® Device Services 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**.

Avaya Aura® Device Services displays the Software Update Deployment page.

2. On the bottom of the Software Update Deployment page, click an entry in the table.

Avaya Aura® Device Services displays the Edit appcast item page.

3. Click **Delete**.

Avaya Aura® Device Services displays the Delete item page.

4. Click **Yes**.

Reviewing download statistics

About this task

The Download statistics table shows the total number of Avaya Workplace Client 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 245.

Download statistics field descriptions

Name	Description
OS	The platform of the Avaya Workplace Client installer.
Fresh Install	The total number of fresh installation attempts for Avaya Workplace Client for the given OS using the Web Deployment service.
Updates	The total number of attempts to update the Avaya Workplace Client soft phones for the given OS using the Web Deployment service.
Total	The total number of fresh installation and update attempts for the Avaya Workplace Client soft phones for the given OS using the Web Deployment service.

Chapter 10: Utility Server administration

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
- Microsoft Edge

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.

Supported and unsupported phone models

Supported phone models

The following table shows phone models and firmware types that you can use with the Avaya Aura® Device Services Utility Server.

Phone model	Supported firmware type		Notes
	SIP firmware	H.323 firmware	
Avaya 96X0 Deskphones			
9620L	✓	✓	You can only use one firmware type at a time. For example, if you want to use SIP firmware, you must deactivate H.323 firmware.
9640	✓	✓	
9640G	✓	✓	
9650	✓	✓	
Avaya 96X1 Deskphones			
9601	✓	✓	—
9608G	✓	✓	
9611G	✓	✓	
9621G	✓	✓	
9641G	✓	✓	
Avaya J100 Series IP Phones			

Phone model	Supported firmware type		Notes
	SIP firmware	H.323 firmware	
J129	✓	✗	—
J139	✓	✗	
J169	✓	✓	
J179	✓	✓	
Avaya Vantage™			
K165	✓	✗	—
K175	✓	✗	
K155	✓	✗	
Avaya 46xx Phones			
4610	✗	✓	Locate the 46xxsettings.txt in the root /var/www/html directory only. The 46xxupgrade file must have the .scr extension, for example, 46xxupgrade.scr.
4620	✗	✓	
4622	✗	✓	
4624	✗	✓	
Avaya 16xx Phones			
1616	✗	✓	The 16xxupgrade.txt file is only supported. Settings or firmware files are not supported.

Unsupported phone models

The Avaya Aura® Device Services Utility Server does not support the 9620 deskphones.

The Avaya Aura® Device Services Utility Server does not support the 7434ND+, 6424D+, 6408D+, 2420D digital phones.

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:

```
"TLSSRV=<Utility Server IP address or
FQDN>,TLSPORT=1543,TLSSRVID=0,HTTPSRV=<Utility Server IP address or
FQDN>,HTTPPORT=80,MCIPADD=<H.323 call server address list>"
```

For example:

```
"TLSSRV=1.2.3.4,TLSPORT=1543,TLSSRVID=0,HTTPSRV=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 HTTPSRV 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/admn055.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.

Enabling access to the Utility Server using an HTTP connection

About this task

By default, you can access files stored on the Utility Server using a secure HTTPS connection. Use this procedure if you want to access the Utility Server using an unsecure HTTP connection.

Before you begin

For AWS deployments, ensure that an inbound rule for HTTP port 80 is configured on a security group that you use for Utility Server IP addresses.

Procedure

In a cluster environment, perform this procedure on the seed node first and then on all non-seed nodes.

1. Log in to the node using an SSH connection.
2. Run the following command to navigate to the `misc` directory:

```
cdto misc
```

3. Run the following command to enable HTTP access:

```
sudo ./us-http-port.sh --enable
```

4. When the configuration process is complete, reload the firewall.

Result

After HTTP access to the Utility Server is enabled on all nodes, you can access Utility Server files, such as `46xxsettings.txt`, using the following URL:

```
http://<Utility Server FQDN>/<file name>
```

For example: `http://utilityserver.example.com/46xxsettings.txt`

Logging in to the Utility Server

About this task

Use this procedure to log in to the Utility Server web administration portal. The portal becomes available after you enable the Utility Server during the Avaya Aura® Device Services installation or upgrade.

You must use the IP address of an Avaya Aura® Device Services node to log in to the Utility Server web administration portal. You *cannot* use virtual IPs addresses of the Utility Server or Avaya Aura® Device Services to log in to the portal.

In a cluster environment, you can use the IP address of any cluster node. If IPv6 support is enabled, you can use either IPv4 or IPv6 addresses.

Procedure

1. Open the Google Chrome or Internet Explorer browser.
2. Navigate to `https://<IP_address>:8543/admin.html`.
In this URL, `<IP_address>` is the IP address of an Avaya Aura® Device Services node.
The following are URL examples:
 - IPv4 address example: `https://192.0.2.44:8543/admin.html`
 - IPv6 address example: `https://[2001:db8::7334]:8543/admin.html`
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 326

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.

- To check the amount of space occupied by uploaded firmware `.zip` files, run the following command:

```
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:

```
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.

Increasing the file size limit for phone firmware packages to 1.5 GB

About this task

By default, the Utility Server supports uploading phone firmware packages no larger than 800 MB. You can increase this limit to 1,500 MB (1.5 GB) if required. For example, when you use Avaya Vantage™ phones in your deployment, as Avaya Vantage™ firmware packages often exceed 800 MB.

! Important:

After upgrading, Avaya Aura® Device Services resets the file size limit to its default value. Therefore, you must repeat this procedure after upgrading Avaya Aura® Device Services.

Procedure

1. Log in to Avaya Aura® Device Services as an administrator using an SSH connection.
2. Run the following command:

```
cdto misc
```

3. To increase the file size limit, run the following command:

```
sudo ./enableVantageFWSupport.sh --install
```

Although the script name references Avaya Vantage™, the script increases the firmware package size limit for *all* phone models that the Utility Server supports.

4. In a cluster environment, repeat the steps above on all remaining nodes in the cluster.
5. To ensure that Avaya Aura® Device Services applied the changes, run the following command:

```
sudo ./enableVantageFWSupport.sh --status
```

Related links

[enableVantageFWSupport.sh command](#) on page 463

[Cannot upload phone firmware packages larger than 800 MB to the Utility Server after the upgrade](#) on page 409

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.

For Avaya 46XX Phones firmware upgrade, the 46xxupgrade file must have the .scr extension, for example, 46xxupgrade.scr.

For Avaya 16XX Phones, use the `16xxupgrade.txt` file. Settings or firmware files are not supported.

! 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 249.
- 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 251.

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.

Related links

[Increasing the file size limit for phone firmware packages to 1.5 GB](#) on page 252

Uploading settings file to the Utility Server

About this task

When you use the Utility Server to manage settings for endpoints, you can manually upload settings file, such as `46xxsettings.txt`, to the Utility Server. If you want to use a `46xxsettings.txt` file containing conditional statements, such as `IF` or `GOTO` commands, use this procedure to manually upload the settings file to the Utility Server. `46xxsettings.txt` files that you generate using the Dynamic Configuration service, do not support conditional statements.

The Utility Server is not clustered in an Avaya Aura® Device Services cluster environment. In a cluster environment, upload a settings file on each cluster node separately. Perform this procedure on the seed node first and then on all non-seed nodes.

Procedure

1. On web browser, enter https://aads_ip_or_fqdn:8543/admin.html
2. On the Utility Server web interface, in the navigation pane, click **IP Phone Custom File Upload**.
3. On the **IP Phone Custom File Upload** screen, click **choose file**.
4. Select the required file and click **Upload Custom Files and Activate**. The file gets uploaded to `/var/www/html/custom`.

Result

After you upload the settings file to all Avaya Aura® Device Services nodes, you can access it from the following URL:

`https://<Utility Server FQDN>/<settings file>`

For example: `https://utilityserver.example.com/46xxsettings.txt`

Related links

[Publishing the configuration settings](#) on page 276

[Administration of the Dynamic Configuration service](#) on page 265

Uploading an IP phone custom file

About this task

Use this procedure to upload custom files, settings, firmware upgrade 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 just after uploading. The Utility Server overwrites existing files.

The Utility Server stores uploaded custom files in the `/var/www/html/custom` directory. However, the uploaded files are available from the `/var/www/html` directory through symbolic links.

Note:

The new script `accessToCustomDir.sh` has been added to **misc** folder to provide an access to utility server `/var/www/html/custom` directory. It will enable users to remove unwanted files or folders from `/var/www/html/custom` directory.

```
cdto misc
sudo ./accessToCustomDir.sh help
```

Using linux command:

```
sudo ./accessToCustomDir.sh ls, to list files from /var/www/html/custom directory
sudo ./accessToCustomDir.sh rm <filename>, to remove a single file
```

```
sudo ./accessToCustomDir.sh "rm <filename*>", to remove multiple files with wild
char *
```

Example:

```
sudo ./accessToCustomDir.sh rm testfile.txt
sudo ./accessToCustomDir.sh "rm *.txt"
```

Before you begin

Configure a DHCP server. For more information, see [Setting up a DHCP server](#) on page 249.

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 in the `/var/www/http/PhoneBackup/` directory. The name of this file contains the extension number of the phone. In a cluster environment, phone settings are stored on the seed node. The Utility Server supports both HTTP and HTTPS authentication methods for backup operations.

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 249.
- For AWS deployments, ensure that an inbound rule for HTTP port 80 is configured on a security group that you use for Avaya Aura® Device Services nodes.

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 one of the following entries to the `46xxsettings.txt` file for the phone model:

- `SET BRURI http://<username>:<password>@<AADS_IP_OR_FQDN>/PhoneBackup`
- `SET BRURI https://<username>:<password>@<AADS_IP_OR_FQDN>/PhoneBackup`

In these entries, `<username>` and `<password>` are credentials of the administrative user that you created during the OVA deployment and `<AADS_IP_OR_FQDN>` is either the IP address or FQDN of Avaya Aura® Device Services. In a cluster environment, `<AADS_IP_OR_FQDN>` is either the IP address or FQDN of the seed node.

PhoneBackup Feature Configuration

This utility script **fixPhoneBackupDos.sh** provides configuration options to manage the PhoneBackup feature, enhancing security and deployment flexibility. It supports the following modes:

- **Disable PhoneBackup:** Suitable for environments using only SIP phones that do not require PhoneBackup functionality.
- **Whitelist Custom IP Ranges :** Allows administrators to restrict access to the PhoneBackup service to trusted IP addresses, such as enterprise proxy CIDR ranges.

Note:

This utility script includes rollback support, enabling safe reversion to previous settings if necessary.

Disabling PhoneBackup Feature or Whitelist Custom IP Range

About this task

Use this procedure to disable PhoneBackup feature or whitelist Custom IP range.

Procedure

1. Open a terminal, navigate to the directory containing the utility script, and run the following command:
`cdto misc`
2. To execute the utility script with the install flag, run the following command
`sudo ./fixPhoneBackupDos.sh --install`
3. When prompted, choose one of the following options:
 - **Block PhoneBackup Feature:** Disables the PhoneBackup feature completely.
 - **Keep PhoneBackup feature by whitelisting an IP from where the PhoneBackup requests emanate:** You are prompted to enter one or more IP subnets (in CIDR notation). Only traffic from these IPs are allowed; All other sources are blocked.

Verifying the Configuration Status of PhoneBackup

About this task

Use this procedure to check the current configuration status of PhoneBackup feature.

Procedure

To check the current configuration status of the PhoneBackup feature, run the following command:

```
sudo ./fixPhoneBackupDos.sh --status
```

Rolling Back Changes in PhoneBackup Feature

About this task

Use this procedure to revert all the changes in the PhoneBackup that are modified by utility script.

Procedure

To revert all the changes in the PhoneBackup that are modified by the utility script, run the following command:

```
sudo ./fixPhoneBackupDos.sh --rollback
```

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 269. 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 Utility Server 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 260.

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

Firmware package statuses

Status	Description
Packed	The firmware package is uploaded on the Utility Server. When the firmware package has this status, you can perform the following actions: • View information about the package. • Unpack the package. • Remove the .zip archive with the package from the Utility Server.
Unpacked	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/<package_name></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/<package_name></code> directory. The .zip archive with the firmware package will still be available on the Utility Server.

Status	Description
Active	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.

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. 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 262

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. To open the required upgrade file in the vi text editor, run the following command:

```
sudo vi /var/www/html/<UPGRADE_FILE>
```

In this command, <UPGRADE_FILE> is the upgrade file name. For example, to open the upgrade file for 96x1 series phones, run the following command:

```
sudo vi /var/www/html/96x1Hupgrade.txt
```

3. 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.

4. Save the upgrade file.

Related links

[Activating a firmware package](#) on page 262

[Assigning a group identifier to a phone model](#) on page 269

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 Utility Server.

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 11: Administration of the Dynamic Configuration service

With the Dynamic Configuration service, Avaya Aura® Device Services can dynamically retrieve and deploy automatic configuration settings on Avaya Workplace Client. 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.
- Avaya 9600 Series IP Deskphones.

Avaya Aura® Device Services generates a separate `46xxsettings.txt` file for each endpoint category. The 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:

- **Global:** Any other settings category can override global settings. Global settings are used for both Avaya Workplace Client and desk phones.
- **Group:** User, platform, exception, and System Manager settings can override group settings. Group settings are only used for Avaya Workplace Client.

When a 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.

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.

- **User:** Platform, exception, and System Manager settings can override user settings. These settings are only used for Avaya Workplace Client.
- **Platform:** Exception and System Manager settings can override platform settings. These settings are only used for Avaya Workplace Client.
- **Exception:** Exception settings are specific to the System Manager Home location. These settings are only used for Avaya Workplace Client.

The Exception settings are not applicable if you use Avaya Aura® Device Services in an environment without Avaya Aura®.

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

Conflicting group names

Do not publish group settings to LDAP groups if there are users that belong to more than one group. Otherwise, a conflict occurs where the same setting is in two different groups with different values. In this case, Avaya Aura® Device Services must choose one value to return and the mechanism used is based on the ASCII ordering of group names, which could result in users getting the wrong value assigned to them for conflicting settings.

When there is a conflict between two group names, Avaya Aura® Device Services does the following to determine which group name to choose:

1. Finds the first character in the group names that differ.

This check is case-sensitive.

2. Determines the unicode decimal representation of the characters.

Avaya Aura® Device Services chooses the group name where the character with a unicode decimal representation is the smallest.

When there is a conflict with more than two groups, Avaya Aura® Device Services uses the same algorithm, but it looks at additional characters.

For example, a company has the following LDAP groups:

- All Users
- HR
- Payroll
- atlanta
- 101_department

In this example, PHNLLENGTH is published to both the 101_department and Payroll groups with a value of 7 and 11 respectively. Avaya Aura® Device Services returns the value 11 from the 101_department group. This is because the unicode decimal representation for the number 1 is 49, and the decimal representation for the capital letter P is 80.

The typical unicode representation flow is numbers (0 to 9) > capital letters > lowercase letters.

Conferencing settings

Avaya Aura® Device Services automatically discovers the following settings from the Avaya Meetings Server during Avaya Workplace Client deployment:

- CONFERENCE_FACTORY_URI
- CONFERENCE_PORTAL_URI
- UNIFIEDPORTALENABLED

You can override the values for these settings from the Avaya Aura® Device Services web administration portal with any fixed user, group, phone model, or platform value.

Automatic discovery

Avaya Workplace Client supports discovery of the following settings:

- Installation parameters as part of the installation process in MS Windows and macOS operating systems.
- Active Directory Group Policy in MS Windows operating system only.
- Configuration discovery via *equinox cloud client* public parameters on `accounts.avayacloud.com`.
- Configuration discovery via DNS SRV record.

For more information about setting up automatic configuration on Avaya Workplace Client, see *Planning for and Administering Avaya Workplace Client for Android, iOS, Mac, and Windows*.

Related links

[Adding a new enterprise LDAP server](#) on page 184

[Dynamic configuration setting priorities](#) on page 268

Considerations for administering SIP parameters in an environment without Avaya Aura®

In Avaya Aura® deployments, Avaya Aura® Device Services obtains SIP parameters, such as SIPDOMAIN or SIP_CONTROLLER_LIST, from System Manager and passes these parameters to SIP clients. Therefore, you do not need to configure these parameters manually. In an environment without Avaya Aura®, Avaya Aura® Device Services does not interact with System Manager and, therefore, cannot obtain SIP parameters automatically. If you use SIP clients in an environment without Avaya Aura® and use Avaya Aura® Device Services to provide configuration parameters to these clients, you must manually configure and publish SIP parameters required for these clients. You must:

- Configure the required SIP parameters on the USER level.
- Publish the parameters for each SIP account separately.

 Note:

Different SIP clients require different SIP parameters. For more information about SIP parameters required for a SIP client, see the *Administering* document for this client.

Viewing the Home location in System Manager

About this task

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

Use this procedure to find the Home location for a user.

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 Home location is displayed in the Call Routing Settings section.

Dynamic configuration setting priorities

With dynamic configuration, different settings that are common at the user, group, platform, global, phone model, and exceptions levels have different priorities.

Avaya Workplace Client

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

- System Manager
- Exception
- 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.

*** Note:**

If you use Avaya Aura® Device Services in an environment without Avaya Aura®, System Manager and Exception settings are not applicable.

Other endpoints and phones

For Avaya J100 Series IP Phones, Avaya 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.

The automatic configuration functionality is only available for supported models of Avaya 9600 Series IP Deskphones, Avaya J100 Series IP Phones, and Avaya Vantage™. Avaya Aura® Device Services does not generate `46xxsettings.txt` files for other phone models.

*** 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** field, provide a unique identifier for each phone model.
A group identifier must be an integer between 0 to 999.
3. Click **Save**.

Adding a new platform

About this task

Avaya Aura® Device Services provides the following pre-defined platform types for which you can publish configuration settings:

- Android
- iOS
- Mac
- Avaya Vantage™
- Windows

If you want to use the dynamic configuration service for clients on another platform, use this procedure to add the platform to Avaya Aura® Device Services.

Procedure

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

Avaya Aura® Device Services displays a list of available platforms.

2. Click **Add**.
3. In **Platform Name**, provide a name for your platform.
4. In **User Agent Identifier**, provide an entry that Avaya Aura® Device Services will use to identify the client platform.

The entry must comply with the following requirements:

- The entry must be part of the User Agent request header that the client platform sends to Avaya Aura® Device Services using Auto Config API.
- The entry must be unique.
- The entry must not be part of a User Agent request header of any other client.
- The entry must not be part or must not contain **User Agent Identifier** configured for any other platform.
- The entry must not be part or must not contain the name of a pre-defined platform.

If you leave **User Agent Identifier** blank, Avaya Aura® Device Services will use the value that you provided in **Platform Name** as the user agent identifier.

5. Click **Save**.

Deleting a platform

About this task

Use this procedure to delete a platform that you added. You cannot delete pre-defined platforms.

When you delete a custom platform, Avaya Aura® Device Services also deletes all settings published for this platform.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Dynamic Configuration > Configure Platforms**.
2. Navigate to the platform you want to delete.
3. Select the check box to the left of the platform name.
4. Click **Delete**.

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

Name	Description
Search Criteria	
Configuration	Displays the USER , Group , Platform , Global , and Exceptions settings for the selected configuration.
User	Displays the Settings configured on SMGR , USER , Group , Platform , Global , and Exceptions settings for the user.

Name	Description
Group	Displays the Group , Platform , and Global settings for the selected group.
Phone Model	Displays the Phone Model settings for the selected phone model.
Platform	Specifies a platform to retrieve the data. • ACML • Android • iOS • Mac • Vantage • Windows • Other platforms defined by you
USER, Group, Platform, Global, Phone Model, and Exceptions	
Search	Searches the setting name from the list of settings for the typed search string.
Include	Includes or excludes the setting.
Setting	Displays a list of settings.
Value	Specifies the value that is assigned to a setting.
Discovered	The system displays this section for the users. Displays the read-only settings. To edit the values, go to the SMGR configuration.

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

Link	Description
View Published Settings	Displays all the published settings for Global, Group, User, Platform, Phone Model, and Exceptions.

Configuration settings

The System Manager specific settings, such as, SIP_CONTROLLER_LIST, SIPDOMAIN, ESMSRVR, 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 Workplace Client 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 Workplace Client for Android, iOS, Mac, and Windows*.

Password masking

For security reasons, Avaya Aura® Device Services does not display the actual values for configuration settings that represent passwords. Avaya Aura® Device Services hides the values for the following settings:

- SIPPASSWORD
- SSOPASSWORD
- ESMPASSWORD
- ACSPASSWORD
- CESPASSWORD
- DIRPASSWORD
- PKCS12PASSWORD
- SCEPPASSWORD
- EWSPASSWORD
- UNIFIED_PORTAL_PASSWORD
- ADMIN_PASSWORD
- AGENT_PASSWORD
- FORCE_SIP_PASSWORD

- SIPHA1
- CESVMPIN
- MYCERT_PASSWORD
- MYCERT_CA_PASSWORD
- DEBUG_REPORT_PASSWORD
- PROCPSWD
- Any custom parameters that are used as passwords.

After you set the values for these settings and save the configuration, Avaya Aura® Device Services displays the special value ***** both on the web administration portal and in the browser developer or inspect view.

In search results, Avaya Aura® Device Services displays password type settings as follows:

- If a setting is editable, then Avaya Aura® Device Services does not display a specific value. If you want to save or publish a configuration, you must set the actual values for the required password type settings. Avaya Aura® Device Services notifies you about this by displaying a warning message at the top of the Configuration page.
- If a setting is not editable, then Avaya Aura® Device Services displays the special value *****. Non-editable settings are auto-discovered from other sources. Avaya Aura® Device Services displays these settings on the Discovered tab when you search settings for a user.

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 Workplace Client for Android, iOS, Mac, and Windows*.

Avaya Aura® Device Services does *not* use these parameters in an environment without Avaya Aura®.

SIP parameters

Name	Description	Avaya Workplace Client platform support
COMM_ADDR_HANDLE_TYPE	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. Avaya Aura® Device Services 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	Supported only on Avaya Aura® Device Services.

Name	Description	Avaya Workplace Client platform support
	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.	
COMM_ADDR_HANDLE_LENGTH	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. The valid value is a positive integer number that contains up to 255 digits. For example, 2000 is a valid value because it contains four digits, which is less than 255.	Supported only on Avaya Aura® Device Services.

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.

 Note:

You cannot set the special value ***** for password type configuration settings when overwriting an existing configuration. If you enter ***** , Avaya Aura® Device Services does *not* consider the value changed.

3. Click **Save**.

4. In the Save Configuration window, select **Overwrite existing configuration** and select an existing configuration.
5. Click **Save**.

Avaya Aura® Device Services 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**.

Avaya Aura® Device Services 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.

Avaya Aura® Device Services does *not* hide values of configuration settings that represent passwords.

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.
- Avaya Aura® Device Services generates `46xxsettings.txt` files only for supported models of Avaya 9600 Series IP Deskphones, Avaya J100 Series IP Phones. If you want to use a `46xxsettings.txt` file that contains configuration for other supported models, you must manually upload it to the Utility Server. For more information, see [Uploading settings file to the Utility Server](#) on page 253 and [Uploading an IP phone custom file](#) on page 254.
- Avaya Aura® Device Services cannot generate `46xxsettings.txt` files that contain conditionals, such as `IF` or `GOTO` commands. If you want to use a `46xxsettings.txt` file that contains conditionals, you must manually upload it to the Utility Server. For more information, see [Uploading settings file to the Utility Server](#) on page 253.
- 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 276.

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**.
Avaya Aura® Device Services 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, Avaya Aura® Device Services applies the settings.

Related links

[Uploading settings file to the Utility Server](#) on page 253

[Administration of the Dynamic Configuration service](#) on page 265

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.

For password type configuration settings, Avaya Aura® Device Services displays the special value *****.

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, select **Group Name** to view the 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, Avaya Aura® Device Services 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 these 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**.

Avaya Aura® Device Services 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 Workplace 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`.
- If you are planning to import configuration settings that represent passwords, ensure that you:
 - Set the data type to “String” for all these settings. Settings that belong to the “PASSWORD” category do not support other data types.
 - Set the “category” attribute to “PASSWORD” for all these settings.

Note:

The “category” attribute is only required for settings that represent passwords. “PASSWORD” is the only supported value for this attribute.

For more information about the JSON file structure, see [JSON file structure](#) on page 280.

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 to 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).

JSON file structure

The following table shows attributes that are used in a JSON file to describe dynamic configuration settings:

Attribute	Description
name	The name of the setting.
description	The description of the setting. Avaya Aura® Device Services displays the description when you hover your mouse over the setting name. If you do not want to provide a description for the setting, set description to "".
type	The data type of the setting. Settings that represent passwords must have the “String” type.

Attribute	Description
default_value	The default value of the setting. If you do not want to provide a default value, set default_value to "".
version	The version of the setting. The default version for settings available on Avaya Aura® Device Services. Therefore, you must set the version value for any setting that you import to Avaya Aura® Device Services as follows: • Less than 100 if the setting is introduced as a new setting. • More than 100 if the setting overwrites any existing setting. The version value must be higher than the values used in previous imports.
category	The attribute that indicates that the setting represents a password. Avaya Aura® Device Services hides the actual values of these settings on the Avaya Aura® Device Services web administration portal. For settings that represent passwords, you must include this attribute and set it to "PASSWORD". Do not use this attribute for other settings.

The following example shows a JSON file containing the following two settings:

- DYNAMIC_SETTING_PASSWORD: Configuration setting that represents a password.
- DYNAMIC_SETTING_NON_PASSWORD: Non-password configuration settings.

```
{
  "settings": [
    {
      "name": "DYNAMIC_SETTING_PASSWORD",
      "description": "This is a setting that is used as a password.",
      "type": "String",
      "default_value": "password12345",
      "version": "2",
      "category": "PASSWORD"
    },
    {
      "name": "DYNAMIC_SETTING_NON_PASSWORD",
      "description": "This is a non-password setting of integer type.",
      "type": "Integer",
      "default_value": "8443",
      "version": "50"
    }
  ]
}
```

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**.
3. On the Import dynamic configuration settings page, in the **Select type of import** field, select **Import 46xxsettings file**.
4. Click **Browse** and select the file that you want to import.
5. Click **Import**.

Avaya Aura® Device Services 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 be in the following format: {CATEGORY}; {SUB-CATEGORY}; {SETTING_NAME}; {SETTING_VALUE}.

The following table describes bulk settings that you can use:

Settings	Description
CATEGORY	The high-level category to which the particular setting belongs. The categories are: • USER • GLOBAL • GROUP • PLATFORM • PHONEMODEL • EXCEPTION
{SUB-CATEGORY}	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. • For the GROUP category, the subcategory is a group name. You can retrieve the group name from LDAP Server.

Settings	Description
	For example: GROUP;Group 1;SUPPORTEMAIL;admin@mysite.com - For the USER category, the subcategory is a user name. The setting name is ESMUSERNAME. For example: USER;user1@mysite.com;CESUSERNAME;user1@mysite.com - For the PLATFORM category, the subcategory is a platform name. The options are Mac, Windows, Android, and iOS. For example: PLATFORM;Windows;APPCAST_URL;https://appcast.mysite.com - For the PHONEMODEL category, the subcategory is a phone model. The options are J1XX, Vantage, and 96XX. For example: PHONEMODEL;J1XX;ADMIN_CHOICE_RINGTONE;Default - For the GLOBAL category, there is no subcategory. The format is: {CATEGORY};{SETTING_NAME};{SETTING_VALUE} For example: GLOBAL;CESSECURE;1 - For the EXCEPTION category, the format is: {CATEGORY};{SOURCE};{EXCEPTION_CONDITION_NAME};{EXCEPTION_CONDITION_VALUE};{SETTING_NAME};{SETTING_VALUE}. 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;location 1;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 `SEMICOLON;GROUP`, use the following:
`GROUP;"SEMICOLON;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 a backslash character as follows: `\"`

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

- Use the pound sign (#) 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.

Avaya Aura® Device Services displays the import status at the top of the page.

When the import is successful, Avaya Aura® Device Services 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, Avaya Aura® Device Services 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

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

Button	Description
Browse	Enables you to select a file in the .csv format for importing the bulk configuration settings.
Import	Imports the added entry or the file and displays the status at the top of the page. When an import action is already in progress and you try to attempt a new bulk import, the system displays the message: Bulk Import is already in progress.
Status	Displays the bulk import status.
Reset	Resets the added entry and clears the text box.

Managing automatic logging in to Avaya clients

About this task

Use this procedure to allow or disallow users to log in to their devices using passwords stored on Avaya Aura® Device Services.

If this feature is enabled, then the following settings are sent in Dynamic Configuration responses:

- SIPHA1
- SIPPASSWORD
- AGENT_PASSWORD

Avaya clients use these SIP credentials for unified login.

 Note:

This feature does not apply to other password settings.

Before you begin

If you are planning to send SIPHA1, SIPPASSWORD, or AGENT_PASSWORD in Dynamic Configuration responses, ensure that these settings are published. Dynamic Configuration responses do not contain not published settings. For more information, see [Publishing the configuration settings](#) on page 276.

Procedure

1. On the Avaya Aura® Device Services web administration portal, in the left navigation pane, navigate to **Dynamic Configuration > Default**.
2. Do one of the following:
 - Select the **Allow passwords** check box to send the settings in Dynamic Configuration responses.
 - Clear the **Allow passwords** check box to disable sending the settings in Dynamic Configuration responses.
3. Click **Save**.

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

Name	Description
Allow passwords	Specifies that the user can log in to the device with the stored password on the server. - If you select the check box, the Dynamic Configuration response contains the SIPHA1, SIPPASSWORD, and AGENT_PASSWORD settings. Avaya clients use these SIP credentials for unified login.  Note: If the Allow passwords check box is selected but the settings are not published, then the Dynamic Configuration response will not contain these settings. For more information about publishing settings, see Publishing the configuration settings on page 276. - If you clear the check box, the Dynamic Configuration response does not contain the SIPHA1, SIPPASSWORD, and AGENT_PASSWORD settings.
Lock Settings	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 Lock Settings check box, the system displays the Obscure locked settings check box.
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.

Button	Description
Save	Saves the default configuration settings.
Cancel	Resets any changes made on the page.

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**.
Avaya Aura® Device Services displays the Split Horizon DNS Mapping page.
3. Click **Add**.
Avaya Aura® Device Services 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**.
Avaya Aura® Device Services displays the Split Horizon DNS Mapping page.
3. Select the **Enable Split Horizon DNS Mappings** check box.

Split Horizon DNS Mapping field descriptions

Name	Description
Search	Searches the values from the list of entries for the typed search string.
IP Address	Specifies the IP address of the different servers or URLs to which the client will connect.
Fully Qualified Domain Name	Specifies the fully qualified domain name of the different servers or URLs to which the client will connect.

Button	Description
Add	Displays a row to specify the IP address and FQDN of the different servers or URLs to which the client will connect.
Save	Saves the added row entry.
Cancel	Discards any changes made on the page.

Chapter 12: 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.

Avaya Aura® Device Services supports IWA for multiple domains. The User Principal Name (UPN) domain and the authentication domain must be the same as the root domain of the directory.

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 Workplace Client 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 is mapped to the Service Principal Name (SPN) of the Avaya Aura® Device Services server.
- Domain users for all individual users.
- 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 `<domain>\<user name>`.

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:

- Do not change the userPrincipalName attribute configured for the user. If you change the userPrincipalName after IWA is configured, IWA will not work.
- The Active Directory, Windows client, and Avaya Aura® Device Services server must resolve each other 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, track of any SPNs assigned to users.

Avaya Aura® Device Services supports IWA for multiple domains. To configure IWA for multiple domains that are in different Active Directories, repeat this procedure on each Active Directory.

! Important:

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

- The hostname used to access the Tomcat server must match the host name in the SPN exactly. Otherwise, authentication fails.
- 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`.
- Avaya Aura® Device Services supports IWA for parent and child domains. However, you cannot assign an SPN and generate a `tomcat.keytab` file for the child domain because the SPN can only be mapped to a single user in a forest. Here, you need to assign the SPN and generate a `tomcat.keytab` file for the parent domain.

Procedure

1. Create a new IWA service account.

Do not select an account associated with an existing user.

2. Run the following command to attach the SPN to the domain name:

```
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`:

```
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 292.
3. **(Optional)** To remove a duplicated SPN from another user, run the following command:

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

4. Run one of the following commands to generate a `tomcat.keytab` file:

- If FIPS is disabled on Avaya Aura® Device Services, run the following command:

```
ktpass /out c:\tomcat.keytab /mapuser <Domain User  
Login>@<Kerberos realm> /princ HTTP/<FRONT-END FQDN>@<Kerberos  
realm> /ptype KRB5_NT_PRINCIPAL /pass +rndPass /crypto all /kvno  
0
```

- If FIPS is enabled on Avaya Aura® Device Services, run the following command:

```
ktpass /out c:\tomcat.keytab /mapuser <Domain User  
Login>@<Kerberos realm> /princ HTTP/<FRONT-END FQDN>@<Kerberos  
realm> /ptype KRB5_NT_PRINCIPAL /pass +rndPass /crypto  
<Encryption Type> /kvno 0
```

Where <Encryption Type> can be one of the following:

- AES256-SHA1: If you want to use the AES256-SHA1 encryption type.
- AES128-SHA1: If you want to use the AES128-SHA1 encryption type.

The encryption type must correspond to the encryption type configured for the domain user that is mapped to the Avaya Aura® Device Services SPN. For more information, see [Enabling encryption for the domain user](#) on page 293.

AES256-SHA1 is the preferred encryption type.

The following example displays the command for generating a keytab file in FIPS mode. In this 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_spn_user@EXAMPLE.COM /princ HTTP/
aads.example.com@EXAMPLE.COM /ptype KRB5_NT_PRINCIPAL /pass +rndPass /crypto
AES256-SHA1 /kvno 0
```

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.

Next steps

- If you are using FIPS, enable AES encryption for the domain user as described in [Enabling encryption for the domain user](#) on page 293.
- Set up IWA on Avaya Aura® Device Services as described in [Setting up IWA on the Avaya Aura Device Services administration portal](#) on page 294.

Related links

[Enabling encryption for the domain user](#) on page 293

Windows Domain Controller command descriptions

[Setting up the Windows Domain Controller](#) on page 291 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.	<code>aads.example.com</code>
<Domain user login>	The Windows login ID for the domain user you created.	<code>aads_spn_user</code>
<Kerberos realm>	The domain name for the Kerberos realm. The Kerberos realm is always the uppercase equivalent of the DNS domain name.	<code>EXAMPLE.COM</code>

Enabling encryption for the domain user

About this task

In FIPS mode, Kerberos uses Advanced Encryption Standard (AES). By default, support for Kerberos AES authentication is disabled for Active Directory users. Use this procedure to enable encryption support for the domain user that is mapped to the Avaya Aura® Device Services SPN.

This procedure is only required if FIPS is enabled on Avaya Aura® Device Services.

Before you begin

Generate a keytab file as described in [Setting up the Windows Domain Controller](#) on page 291.

Procedure

1. In Active Directory, select the domain user that is mapped to the Avaya Aura® Device Services SPN.
For example: aads_spn_user.
2. Open the domain user properties.
3. Click the **Account** tab.
4. In the Account options area, do one of the following:
 - If you used the AES256–SHA1 encryption type when generating a keytab file, select the **This account supports Kerberos AES 256 bit encryption** check box.
 - If you used the AES128–SHA1 encryption type when generating a keytab file, select the **This account supports Kerberos AES 128 bit encryption** check box.
5. Click **OK**.

Related links

[Setting up the Windows Domain Controller](#) on page 291

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.

To configure IWA for multiple domains, you must repeat this procedure for each active directory that requires the use of IWA.

Note:

If you upgrade Avaya Aura® Device Services to a later release, set up IWA, and then downgrade Avaya Aura® Device Services, IWA remains configured and enabled.

Before you begin

Generate a `tomcat.keytab` file for the active directory that you plan to use for IWA. If you want to configure IWA for multiple domains, you must generate a `tomcat.keytab` file for each active directory.

Procedure

1. On the Avaya Aura® Device Services administration portal, click **LDAP Configuration**.
2. Select the required Active Directory.
3. In the Server Address and Credentials area, do the following:

- a. In the **Windows Authentication** 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 you use must be the domain controller with the appropriate Active Directory version as the server type.

4. 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 [4.b](#) on page 295 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.

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

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

Chapter 13: 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 14: Cassandra clustering configuration on Avaya Aura[®] Device Services

In cluster deployments, Cassandra clustering provides redundant storage of SIP device data on Avaya Aura[®] Device Services nodes. To further improve resiliency, you can assign each node to a specific Cassandra datacenter. A datacenter is a logical grouping of Avaya Aura[®] Device Services nodes within the cluster. When you use multiple datacenters, the Cassandra database is replicated on the nodes as follows:

- Each Cassandra datacenter configured in your deployment has its own replica of the Cassandra database.
- Within a Cassandra datacenter, the database is replicated on multiple nodes. The exact number of copies depends on the number of nodes in the datacenter.

Avaya Aura[®] Device Services automatically configures and maintains the replication settings, such as the replication factor, for each datacenter.

By default, all cluster nodes belong to the default Cassandra datacenter, which has the “dc1” name. To assign a node to another datacenter, specify the datacenter name when installing the node or at any time after installation. If you do not select a datacenter during installation, Avaya Aura[®] Device Services assigns the node to the default datacenter. If required, you can move nodes between datacenters.

Note:

A datacenter is a virtual entity. Therefore, to create a new datacenter, you only need to specify a unique datacenter name when installing or configuring a node. Avaya Aura[®] Device Services automatically updates the clustering configuration as appropriate.

By default, Avaya Aura[®] Device Services synchronizes the data between the databases weekly. You can schedule the synchronization on a specific day of the week or disable the synchronization.

Recommendations for configuring Cassandra clustering

Avaya recommends that you:

- Use two Cassandra datacenters in your deployment.

You can configure more than two datacenters, but it might not provide additional redundancy compared to the two datacenters setup.

- Distribute Avaya Aura[®] Device Services nodes evenly between the Cassandra datacenters to balance the load on each datacenter.

- Configure an additional seed node so that:
 - The primary seed node belongs to one datacenter.
 - The additional seed node belongs to another datacenter.

This approach improves bootstrapping the gossip process for new nodes joining the cluster. When you add a new node to a datacenter, this node communicates with the seed node of the datacenter instead of the main seed node of the cluster.

- In a geographically distributed deployment, assign Avaya Aura® Device Services nodes to Cassandra datacenters based on node location. Thus, you minimize the network latency in internode communications.

Considerations

If you upgrade to Release 10.2.x from a previous release, all nodes in your deployment belong to the default “dc1” datacenter. You can configure datacenters as appropriate on the Clustering configuration page of the configuration utility. For more information about re-assigning nodes to datacenters, see Chapter “Cassandra clustering configuration on Avaya Aura® Device Services” in *Administering Avaya Aura® Device Services*.

Related links

[Scheduling a Cassandra database repair](#) on page 43

[Assigning a node to a different Cassandra datacenter](#) on page 300

[Reviewing the Cassandra database status](#) on page 301

[Configuring an additional seed node](#) on page 302

Scheduling a Cassandra database repair

About this task

Avaya Aura® Device Services repairs the Cassandra database weekly to ensure that the information in the database is consistent throughout the nodes. You can select a day of the week when Avaya Aura® Device Services repairs the database or disable the repair process. By default, Avaya Aura® Device Services performs the repair process on Sundays.

Important:

The repair process might impact the Avaya Aura® Device Services performance. Therefore, Avaya recommends that you select the least busy day of the week for your enterprise.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **System Parameters > Parameter Configuration**.
2. In **NODETOOL_REPAIR_MANAGEMENT**, choose one of the following to select when Avaya Aura® Device Services performs the Cassandra database repair:
 - To change the default day of the week for the repair process, select the appropriate day of the week.

- To disable the repair process, select **None**.
3. Click **Save**.

Related links

[Cassandra clustering configuration on Avaya Aura Device Services](#) on page 298

Assigning a node to a different Cassandra datacenter

About this task

To change the structure of your Cassandra datacenters, you can assign an Avaya Aura® Device Services node to a different Cassandra datacenter. For example, after upgrading to Release 10.1.1, all Avaya Aura® Device Services nodes belong to the default datacenter. To improve resiliency, you can re-assign some of the nodes to a new datacenter.

Note:

A datacenter is a virtual entity. Therefore, to create a new datacenter, you only need to specify a unique datacenter name when configuring a node.

Procedure

1. Log in as an administrator to the CLI of the node you want to re-assign to another Cassandra database.
2. To start the configuration utility, run the following command:

```
app configure
```
3. Select **Clustering Configuration** and press `Enter`.
4. Select **New Datacenter name** and press `Enter`.
5. In **Name**, enter the Cassandra datacenter name as follows:
 - To add the node to a new datacenter, provide a name of your choice for that datacenter.
 - To add the node to an existing datacenter, provide the name of one of existing datacenters on Avaya Aura® Device Services.
 - To add the node to the default “dc1” datacenter, leave the field blank.
6. Select **Apply** and press `Enter`.

Avaya Aura® Device Services adds the node to the selected datacenter and updates the datacenter topology.

Related links

[Cassandra clustering configuration on Avaya Aura Device Services](#) on page 298

Reviewing the Cassandra database status

About this task

You can use the `nodetool` command to review the following information about the Cassandra database:

- The status of each Cassandra node.
- The list of Cassandra datacenters.

For example, you can review the Cassandra status after creating a new datacenter to ensure that the datacenter is created successfully.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:

```
nodetool status
```

Avaya Aura® Device Services displays information about the Cassandra database.

Example

The following is an example of the command output for an Avaya Aura® Device Services cluster with two Cassandra datacenters: dc1 and dc2.

```
[admin@aaads bin]$ nodetool status

Datacenter: dc1
=====
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
-- Address      Load          Tokens   Owns    Host
ID                                     Rack
UN  192.0.2.1    3 MiB         256      100.0%  abcdef01-2345-6789-abcd-
ef0123456789  rack1
Datacenter: dc2
=====
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
-- Address      Load          Tokens   Owns    Host
ID                                     Rack
UN  192.0.2.2    2.37 MiB      256      100.0%  01234567-89ab-
cdef-0123-456789abcdef  rack1
```

Related links

[Cassandra clustering configuration on Avaya Aura Device Services](#) on page 298

Configuring an additional seed node

About this task

For internode communication, Cassandra uses a protocol called gossip. To improve bootstrapping the gossip process for new nodes joining the cluster, you can configure an additional seed node so that each Cassandra datacenter in your cluster has one seed node. With this approach, when you add a node to a Cassandra datacenter, this node communicates with the seed node of the datacenter instead of the main seed node.

Note:

You do not need to configure an additional seed node if you use a single Cassandra datacenter in your cluster.

If you configure an additional seed node, you must repeat this procedure on all nodes in the cluster. You must also ensure that you use the same list of additional seed nodes on all nodes in the cluster.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. To start the configuration utility, run the following command:

```
app configure
```
3. Select **Cassandra configuration** and press `Enter`.
4. Select **Additional Seed node IP** and press `Enter`.
5. Type the IP address of the non-seed node in the cluster that you want to make the additional seed node.
6. Select **Save** and press `Enter`.
7. Select **Apply** and press `Enter`.
8. Repeat the steps above on all remaining cluster nodes.

Related links

[Cassandra clustering configuration on Avaya Aura Device Services](#) on page 298

Chapter 15: Security options

Configuring the data retention period

About this task

Log files and the Avaya Aura® Device Services Cassandra database contain private and sensitive user data. To maximize data privacy and security, you can specify how long you want to keep user data on Avaya Aura® Device Services. The default data retention period is 1 day.

Avaya Aura® Device Services encrypts log files that are older than the configured retention period, but it does not delete these logs.

When a user is deleted from data sources, such as the enterprise LDAP directory, iView, or System Manager, Avaya Aura® Device Services deletes the corresponding records for that user from the Cassandra database within the last hour before the configured retention period elapses. For example, if the retention period is one day and the user is just deleted from the LDAP directory, then Avaya Aura® Device Services removes the user information from the Cassandra database within the time range between 23 and 24 hours after the user is deleted from the LDAP directory.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Data Security > Data Retention**.
2. In **Retention time (days)**, set the period for which you want to keep user data on Avaya Aura® Device Services.

The range is 1 to 30 days.

3. Click **Save**.

Related links

[Data retention](#) on page 27

[Log management](#) on page 332

Antivirus support

Avaya Aura® Device Services supports the following antiviruses:

- Microsoft Azure Arc

- Microsoft Defender
- Qualys Cloud Agent

Avaya Aura® Device Services installer does not include any antivirus. If you want to use antivirus software on Avaya Aura® Device Services, you must install it separately. For details about obtaining and installing an antivirus, see the official documentation for the antivirus.

Before installing an antivirus, ensure that Avaya Aura® Device Services meets the prerequisites for antivirus installation.

Related links

[Prerequisites for installing antivirus software](#) on page 304

[Changing the SELinux mode to “permissive”](#) on page 304

Prerequisites for installing antivirus software

If you plan to use antivirus software on Avaya Aura® Device Services, ensure that the following prerequisites are met:

Prerequisites for OVA-based deployments

- Increase the virtual machine RAM memory by 4 GB.

For example, if your virtual machine has 15 GB RAM, increase it by 4 GB to 19 GB RAM in total.

- Change the SELinux mode to “permissive”.

Prerequisites for software-only deployments

- If the current RAM memory of your virtual machine or cloud instance is less than 19 GB, increase it by 4 GB.

For example, if your virtual machine has 16 GB RAM, increase it by 4 GB to 20 GB RAM in total.

- Allocate at least 6 GB of swap space on RHEL.
- Change the SELinux mode to “permissive”.

Related links

[Antivirus support](#) on page 303

[Changing the SELinux mode to “permissive”](#) on page 304

Changing the SELinux mode to “permissive”

About this task

Before installing antivirus software on Avaya Aura® Device Services, you must ensure that the SELinux kernel security module operates in the “permissive” mode.

Before you begin

In OVA-based deployments, contact Avaya support personnel to configure the root password. Avaya Aura® Device Services does not have root access by default in ova-based deployments.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as follows:

- In OVA-based deployments, log in as an administrator, and then switch to the root user using the following command:

```
su root
```

- In software-only deployments, log in as the root user.

2. To set the SELinux mode to “permissive”, run the following command:

```
setenforce 0
```

3. Open SELinux configuration file `/etc/selinux/config` in a text editor.

4. Set the value of the `SELINUX` parameter to `permissive`.

```
SELINUX=permissive
```

Warning:

Ensure that `permissive` is properly spelled. Misspelling the setting value can cause kernel panic issues.

5. Save the file.

6. To reboot Avaya Aura® Device Services, run the following command:

```
reboot
```

7. To verify the SELinux configuration, do the following:

- a. Log in to the Avaya Aura® Device Services CLI as an administrator.
- b. Run the following command:

```
sestatus
```

- c. Ensure that Avaya Aura® Device Services displays `permissive` in the command output.

Related links

[Antivirus support](#) on page 303

[Prerequisites for installing antivirus software](#) on page 304

File access privileges

For security reasons, administrative users cannot modify files owned by the root user using commands such as `chmod`, `rm`, `chown`, or `vi`. Administrative users cannot modify files owned by root even if obtaining root privileges by running commands with `sudo`.

If required, you can modify files owned by root as the sroot user. To obtain the sroot privileges, you must enable the EASG functionality first. After enabling EASG, you can switch to the sroot user by running the following command:

```
su - sroot
```

+ Tip:

You can check the file ownership by running the following command:

```
ls -l <FILENAME>
```

Data encryption management

When you deploy the Avaya Aura® Device Services OVA, you can enable data encryption and configure basic settings, such as providing a passphrase or enabling the local key store. After deploying the Avaya Aura® Device Services OVA, you can use system layer commands to perform additional data encryption management operations, such as the following:

- Enabling a remote key server.
- Managing encryption passphrases.
- Reviewing data encryption status.

! Important:

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

Related links

[Data encryption commands](#) on page 460

Enabling or disabling disk encryption on Avaya Aura® Device Services

About this task

You cannot enable or disable disk encryption by using the Avaya Aura® Device Services web administration portal or the configuration utility. However, you can enable or disable disk encryption when restoring Avaya Aura® Device Services from a backup. This procedure provides the high-level steps for enabling or disabling disk encryption.

! Important:

- This procedure only applies to OVA-based deployments. You cannot enable disk encryption for software-based deployments.
- For AWS deployments, you cannot enable disk encryption on Avaya Aura® Device Services. You must enable disk encryption on AWS itself. For more information, see [How to Protect Data at Rest with Amazon EC2 Instance Store Encryption](#).

This procedure applies to cluster and standalone Avaya Aura® Device Services deployments.

Procedure

1. Perform a full system backup:
 - a. Back up each node of your Avaya Aura® Device Services deployment.
 - b. Record configuration values from the existing Avaya Aura® Device Services system.
 - c. Copy logs, home directory content, and backup files to an external storage.

For more information, see [Backing up Avaya Aura Device Services](#) on page 351.

2. Deploy new virtual machines.

You can enable or disable disk encryption as needed when deploying the Avaya Aura® Device Services OVA. For information about the deployment procedures, see “VMware deployment options” in *Deploying Avaya Aura® Device Services*.

Important:

- You must use the same OVA and the same version of the Avaya Aura® Device Services application that was backed up.
 - You must use the original network settings, such as host names and IP addresses, from the currently installed cluster when deploying new virtual machines.
3. Restore the Avaya Aura® Device Services application using the backups created in step 1.

For information about restoring Avaya Aura® Device Services, see [Restoring Avaya Aura Device Services in a standalone environment](#) on page 358 or [Restoring an Avaya Aura Device Services cluster](#) on page 360.

Remote key server management

When configuring data encryption during the OVA deployment, if you choose not to enter a passphrase after every reboot, Avaya Aura® Device Services stores encryption keys in a local key store. To enhance security, you can set up a remote key server. You can add multiple remote key servers.

Enabling a remote key server

About this task

Use this procedure to use a remote key server to store encryption keys.

When adding a remote key server for the first time, you can choose either to continue using the local key store or to disable it. When both the local key store and the remote key server are enabled at the same time, Avaya Aura® Device Services uses the local key store to decrypt the encrypted disks at boot time.

If you already have a remote key server enabled, you can use this procedure to add another remote key server.

Before you begin

Configure your remote key server. The exact configuration procedure depends on the key server you are using.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:

```
sys encryptionRemoteKey add <server address> <port>
```

In this command:

- <server address> is the IP address or FQDN of the remote key server.
 - <port> is a port that the remote key server uses to connect to Avaya Aura® Device Services. This is an optional value. If you do not enter a port number, the remote key server uses port 80 by default.
3. When prompted, enter the existing passphrase.
 4. When prompted to remove the local key store, do one of the following:
 - To disable the local key store, enter *y*.
 - To continue using the local key store, enter *n*.

Disabling a remote key server

About this task

Use this procedure if you do not want to use a remote key server to store encryption keys. If you have multiple remote key stores, Avaya Aura® Device Services will continue using other remote key stores until you disable them.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:

```
sys encryptionRemoteKey remove <server address>
```

In this command, <server address> is the IP address or FQDN of the remote key server you want to disable. You must use the same IP address or FQDN that you used when enabling the remote key server.

Passphrase management

Avaya Aura® Device Services requires an encryption passphrase to access encrypted partitions.

When enabling data encryption during the Avaya Aura® Device Services OVA deployment, you set up a single passphrase. After the OVA is deployed, you can use system layer commands to:

- Configure up to seven additional passphrases.
- Change existing passphrases.
- Remove a passphrase.
- View status of passphrases.

Adding a passphrase

About this task

Use this procedure to set up additional passphrases. You can have up to seven passphrases in total. If you have multiple passphrases, you can use any of them to access encrypted disk partitions.

A passphrase you add must comply with the passphrase complexity rules.

Before you begin

Ensure that you have a passphrase slot available. For more information, see [Reviewing the passphrase status](#) on page 310.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:

```
sys encryptionPassphrase add
```
3. When prompted, type one of the existing passphrases.
4. When prompted, type a new passphrase.
5. Type the new passphrase again to confirm it.

Passphrase complexity rules

All encryption passphrases you add to Avaya Aura® Device Services must contain at least:

- Eight characters.
- One character from each of the following character sets:
 - Uppercase letters: A to Z
 - Lowercase letters: a to z
 - Numerics: 0 to 9
 - Special characters: !, @, #, %, \$, ^, *, ?, and _

Related links

[passwdrules command](#) on page 458

Removing a passphrase

About this task

Use this task to remove an existing encryption passphrase.

Avaya Aura® Device Services requires at least one encryption passphrase. If you have only one passphrase, you cannot remove it.

Procedure

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

2. Run the following command:

```
sys encryptionPassphrase remove
```

3. When prompted, type the encryption passphrase you want to remove.

Reviewing the passphrase status

About this task

Use this procedure to view information about the number of passphrases you have on Avaya Aura® Device Services.

Tip:

You can use this procedure before adding a new passphrase to see if Avaya Aura® Device Services has a free slot for a new passphrase.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:

```
sys encryptionPassphrase list
```

Avaya Aura® Device Services displays passphrase and slot assignment information.

Slot	Status	Passphrase/Remote Server
Key Slot 0:	ENABLED	Passphrase
Key Slot 1:	ENABLED	Passphrase
Key Slot 2:	ENABLED	Passphrase
Key Slot 3:	DISABLED	empty
Key Slot 4:	DISABLED	empty
Key Slot 5:	DISABLED	empty
Key Slot 6:	DISABLED	empty
Key Slot 7:	DISABLED	empty

Viewing data encryption status

About this task

Use this procedure to view information about data encryption, including the following:

- Whether data encryption is enabled.
- Whether the local key store is enabled.
- Whether the encryption passphrase must be entered after every reboot.
- Information about configured remote key servers.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the `sys encryptionStatus` command.

Local key store management

Enabling the local key store

About this task

If you do not want to enter an encryption passphrase after every Avaya Aura® Device Services reboot and you do not have a remote key server, you can enable the local key store. However, the local key store is less secure than a remote key store or entering a passphrase after every reboot.

You can enable the local key store even if a remote key server is enabled. When both the local key store and the remote key server are enabled at the same time, Avaya Aura® Device Services uses the local key store to decrypt the encrypted disks at boot time.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:

```
sys encryptionLocalKey enable
```
3. When prompted, enter the encryption passphrase.

Disabling the local key store

About this task

When you disable the local key store and do not have a remote key server, you will need to enter your passphrase after every Avaya Aura® Device Services reboot. If at least one remote key server is configured, then Avaya Aura® Device Services will use this remote key server to store encryption keys.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:

```
sys encryptionLocalKey disable
```

Advanced Intrusion Detection Environment tool management

Advanced Intrusion Detection Environment (AIDE) is a tool for monitoring file system changes. AIDE creates a baseline database of system layer files and then verifies the integrity of the files by comparing the database to the actual state of the system layer files. AIDE only performs file integrity checks and does not provide other checks, such as rootkit searches.

! Important:

Software-only deployments do *not* include the AIDE tool. If you want to use AIDE on Avaya Aura® Device Services deployed as a software-only application, you must install AIDE separately.

On Avaya Aura® Device Services, you can manage AIDE using the `fsit.sh` system layer script, which is located in the `/opt/Avaya/bin` directory. The `fsit.sh` script is available after you deploy the Avaya Aura® Device Services OVA.

Avaya recommends that you run AIDE scanning at least once a week.

Creating a baseline database

About this task

Use this procedure to create a baseline database of operational system and Avaya Aura® Device Services files. AIDE uses this database as a reference when performing file system integrity scans.

You must create a database before you start running AIDE scans. Do *not* create a new database before each scan. Create a new baseline after you installed Avaya Aura® Device Services and then create a new baseline each time after you upgraded Avaya Aura® Device Services.

The database creation process can take up to 50 minutes depending on the system data.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to navigate to the `fsit.sh` script location:

```
cd /opt/Avaya/bin
```

3. Run the following command to create an AIDE database as a background process:

```
sudo ./fsit.sh -updateDB &
```

Creating the database as a background process enables you to perform other tasks at the same time.

Result

AIDE creates the baseline database and records the results in the `/var/log/aide/aide_update_status.log` file. If the database is created successfully, the log contains the `Completed` entry and a time stamp. Otherwise, the log contains the `Failed` entry. You can view the log file content using the `cat` command.

The following is an example of the `cat` command output when the baseline database is created successfully.

```
[admin@aads68 bin]$ sudo cat /var/log/aide/aide_update_status.log
Completed (Wed Dec 11 15:27:24 IST 2019)
[admin@aads68 bin]$
```

AIDE scanning

During the scanning process, AIDE compares the actual state of the file system with the reference values stored in the baseline database and informs you if there are any differences. You can either run AIDE scanning manually or configure automatic scanning. AIDE scanning can take up to 50 minutes depending on the system data. AIDE records the scanning results to the `/var/log/aide/aide_scan_status.log` file.

You must run AIDE scans on a regular basis.

Excluding files and directories from AIDE scanning

About this task

By default, AIDE checks the integrity of all Avaya Aura® Device Services files and directories, except for the following:

- `/opt/spirit/LogTail*`
- `/opt/spirit/logging/`
- `/opt/spirit/persist/persisted_ids.properties`

Avaya Aura® Device Services regularly updates certain files and directories, such as `/opt/Avaya/DeviceServices/<version>/logs/`. AIDE includes all changed files in the scanning report, regardless of the reason for the change. This might result in false positive alarms in the scan report. You can add certain files and directories you want to exclude from scanning to the `/etc/aide.conf` AIDE configuration file. AIDE will not include these files and directories in scanning reports.

Warning:

Be cautious when excluding a file or directory from scanning because an intruder might place a malicious file in a place that AIDE does not check.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Open the `/etc/aide.conf` file in a text editor.
For example, to open the file in `vi`, run the `vi /etc/aide.conf` command.
3. For each file or directory you want to exclude from scanning, add an entry in the following format:

```
!<path to file or directory>
```

In this entry, `<path to file or directory>` is the absolute path to the file or directory you want to exclude. For example, enter `!/opt/Avaya/DeviceServices/8.0.1.0001/logs/` to exclude the entire directory from the report.

If you want to exclude a single file, add the `$` character at the end of the entry. For example: `!/opt/Avaya/DeviceServices/8.0.1.0001/logs/File.log$`

The entry format supports regular expressions. For example, you can enter `!/opt/Avaya/DeviceServices/8.0.1.0001/logs/File*` to exclude only files and directories that have names starting with `File`.

4. Save the `/etc/aide.conf` file.

Running AIDE scanning manually

About this task

Use this procedure to run AIDE scanning manually. Scanning can take up to 50 minutes, depending on the system data. Avaya recommends that you run AIDE scanning at least once a week.

Run AIDE scanning during the least busy periods to minimize the impact on Avaya Aura® Device Services performance.

Before you begin

Ensure that you created a baseline database for your current Avaya Aura® Device Services release.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to navigate to the `fsit.sh` script location:

```
cd /opt/Avaya/bin
```

3. Run the following command to run AIDE scanning as a background process:

```
sudo ./fsit.sh -scanNow &
```

Result

AIDE checks the file system integrity and records the results of the scan to the `/var/log/aide/aide_scan_report.log` file.

Next steps

Review the scanning results.

Related links

[Creating a baseline database](#) on page 312

Configuring automatic scanning

About this task

Use this procedure to configure automatic AIDE scanning. Automatic scanning is performed once a day. Scanning can take up to 50 minutes, depending on the system data.

Schedule AIDE scanning for the least busy periods to minimize the impact on Avaya Aura® Device Services performance.

Before you begin

Ensure that you created a baseline database for your current Avaya Aura® Device Services release.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to navigate to the `fsit.sh` script location:

```
cd /opt/Avaya/bin
```

3. Run the following command to configure automatic scanning:

```
sudo ./fsit.sh -enableScan <hour> <minute>
```

Replace `<hour>` and `<minute>` with the time when you want to run the scan process. Use the 24-hour time format. For 12 a.m., enter 0.

For example, enter `sudo ./fsit.sh -enableScan 16 00` to run scanning at 4:00 p.m.

Result

AIDE checks the file system integrity once a day and records the results of the scan to the `/var/log/aide/aide_scan_report.log` file.

Next steps

Review the scanning results.

Related links

[Creating a baseline database](#) on page 312

Disabling automatic scanning

About this task

Use this procedure to disable automatic AIDE scanning.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Run the following command:

```
cd /opt/Avaya/bin
```

3. Run the following command:

```
sudo ./fsit.sh -disableScan
```

Reviewing the AIDE scanning report

About this task

Use this procedure to review the results of the latest AIDE scan. The report contains the following:

- The baseline database status.
- Information about the automatic scanning configuration.
- The last database update and scan dates.
- The number of scanned files and directories.
- The number of added, removed, or changed files.
- Information about added, removed, or changed files.
- Detailed Information about changes.

Procedure

1. Log in to the virtual machine with the deployed Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to navigate to the `fsit.sh` script location:

```
cd /opt/Avaya/bin
```

3. Run the following command:

```
sudo ./fsit.sh -status
```

The scan results are displayed in the terminal window.

Example

The following example shows a scan report with differences between the baseline database and the actual system state found:

```
AIDE 0.15.1 found differences between database and filesystem!!
Start timestamp: 2019-12-11 15:26:52

Summary:
  Total number of files:      55724
  Added files:                0
  Removed files:              0
  Changed files:              1

-----
Changed files:
-----

changed: /opt/Avaya/bin/fsit.sh

-----
Detailed information about changes:
-----

File: /opt/Avaya/bin/fsit.sh
SHA512   : 7v0sOtK9erPSw8dw8GLTCacbvDH028qj , bdxUm2J38kb/1yFDVO/KiA+55CeJlhfx
```

The following example shows a scan report with no differences found:

```
AIDE, version 0.15.1  
### All files match AIDE database. Looks okay!
```

Enabling additional STIG hardening

About this task

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

! Important:

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

* Note:

After you enable additional STIG hardening, ensure that the length of the automatic backup password is at least 15 characters.

Procedure

1. Log in to the virtual machine with the Avaya Aura® Device Services OVA as an administrator.
2. Run the following command to enable additional STIG hardening options:
3. When prompted, press `c` to apply new password rules.
4. **(Optional)** To review the STIG hardening status, run the following command:

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

Disabling additional STIG hardening

About this task

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

Procedure

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

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

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

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

Transport Layer Security overview

Transport Layer Security (TLS) is a protocol designed to secure communications over a network. The TLS protocol provides the following services to all applications:

- Encryption
- Authentication
- Data integrity

Avaya Aura® Device Services supports the following TLS versions:

- 1.2
- 1.3

By default, Avaya Aura® Device Services Release 10.2.x can use either TLS 1.2 or 1.3 when you fresh install the system or migrate from Release 8.1.5. Avaya, recommends, however, that you use TLS 1.3 whenever possible. Advantages of TLS version 1.3 include the following:

- Higher security level to protect users from known attacks.
- Faster TLS handshake.
- The use of cipher suites with no known vulnerabilities.

Considerations and limitations

- Deployment components that interact with Avaya Aura® Device Services over TLS must support the TLS version configured on Avaya Aura® Device Services. Avaya Aura® Device Services uses TLS to interact with the following deployment components:
 - Avaya Aura® System Manager
 - Avaya Aura® Session Manager
 - Avaya Aura® Web Gateway
 - Avaya Aura® Session Border Controller
 - Avaya Meetings Management
 - LDAP server, if secure LDAP connection is enabled
 - External load balancer

For more information about configuring TLS settings on these products, see documentation for the appropriate product.

- Onboard Open LDAP does not support TLS 1.3. If you use Onboard Open LDAP, you must use TLS 1.2.
- System Manager Release 8.x does not support TLS 1.3. If you use System Manager Release 8.x, you must use TLS 1.2.

 Note:

System Manager Release 10.x supports TLS 1.3.

- Switching between TLS versions has no impact on any internal services of Avaya Aura® Device Services services and features enabled on Avaya Aura® Device Services, such as FIPS, Utility Server, or Automatic Configuration.
- Switching between TLS versions might cause considerable Avaya Aura® Device Services downtime because it affects DRS synchronization. Therefore, Avaya recommends that you switch TLS versions during maintenance windows.

Related links

[Selecting a minimum TLS version](#) on page 319

Selecting a minimum TLS version

About this task

You can select a minimum TLS version that Avaya Aura® Device Services uses to establish secure connections. Avaya Aura® Device Services supports TLS versions 1.2 and 1.3.

- If you select version 1.2, Avaya Aura® Device Services can use either TLS 1.2 or 1.3 to establish connections.
- If you select version 1.3, Avaya Aura® Device Services only uses TLS 1.3.

For security reasons, Avaya recommends that you use TLS 1.3 whenever possible.

 Note:

Switching between TLS versions might cause considerable Avaya Aura® Device Services downtime because it affects DRS synchronization. Therefore, Avaya recommends that you switch TLS versions during maintenance windows.

Before you begin

Ensure that all deployment components that interact with Avaya Aura® Device Services over TLS support the TLS version that you plan to select.

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal.
2. Navigate to **Security Settings > TLS Configuration**.
3. In **Minimum TLS version**, select an appropriate TLS version.
4. Click **Save**.

Related links

[Transport Layer Security overview](#) on page 318

Configuring UEFI Secure Boot for OVA-based virtual machines

About this task

Unified Extensible Firmware Interface (UEFI) is an interface between the operating system and the platform firmware that replaces the legacy BIOS interface. Secure Boot is an UEFI feature that secures the operating system boot-up process by preventing the loading of boot loaders and drivers that are not signed with a trusted digital signature.

By default, Avaya Aura® Device Services Release 10.2.x OVA-based deployments have UEFI and Secure Boot enabled. For security reasons, Avaya recommends that you use Secure Boot whenever possible.

For more information about managing Secure Boot settings on VMware virtual machines, see [UEFI Secure Boot](#) in the VMware product documentation.

Before you begin

Deploy a virtual machine.

Procedure

1. Log in to the vSphere Client.
2. Navigate to a Avaya Aura® Device Services virtual machine.
3. Right-click the virtual machine and select **Edit Settings**.
4. Click the **VM Options** tab.
5. Click **Boot Options**.
6. Ensure that **Firmware** is set to **EFI (recommended)**.
7. Do one of the following:
 - To enable Secure Boot, select the **Secure Boot** check box.
 - To disable Secure Boot, clear the **Secure Boot** check box.
8. Click **OK**.

Related links

[Checking the UEFI Secure Boot status](#) on page 320

Checking the UEFI Secure Boot status

About this task

You can check whether the UEFI Secure Boot is enabled on a virtual machine.

Procedure

1. Log in to a virtual machine using an SSH connection.
2. To check the status, run the following command:

```
mokutil --sb-state
```

- If the command output is `SecureBoot enabled`, UEFI Secure Boot is enabled.
- If the command output is `Failed to read SecureBoot`, UEFI Secure Boot is disabled.

Related links

[Configuring UEFI Secure Boot for OVA-based virtual machines](#) on page 320

Configuring the SameSite cookie attribute

About this task

When you use the CORS technology, Avaya Aura® Device Services might receive cross-origin HTTP requests from a different domain. To prevent cross-site request forgery attacks, you can use the SameSite attribute to specify when Avaya Aura® Device Services sends cookies in response to cross-origin requests. The SameSite attribute can have one of the following values:

- **Strict:** Avaya Aura® Device Services only sends cookies to the domain that sent the HTTP request. Avaya Aura® Device Services does not send cookies to third-party domains. It also does not send cookies for cross-origin requests.

Avaya Aura® Device Services uses this values after a fresh installation of Release 8.0.2.

- **Lax:** Avaya Aura® Device Services sends cookies when performing top-level navigations, but does not send cookies for cross-origin requests.

Avaya Aura® Device Services uses this value after upgrading to Release 8.0.2.

- **None:** Avaya Aura® Device Services sends cookies in response to all requests, including cross-origin requests.

You can set the SameSite attribute for the following interface levels.

- Service interface, which is used for REST API and Utility Server cookies.
- Administrator interface, which is used for Avaya Aura® Device Services and Utility Server administration portal cookies.

Avaya Aura® Device Services retains the configured values after an upgrade.

Before you begin

Enable cross-origin resource sharing.

Procedure

1. Do the following to configure the SameSite attribute for the Service interface:
 - a. On the Avaya Aura® Device Services web administration portal, navigate to **Service Connections > CORS Configuration > Service Interface**.
 - b. From **SameSite cookie attribute value**, select **Strict**, **Lax**, or **None**.
 - c. Click **Save**.
2. Do the following to configure the SameSite attribute for the Administrator interface:
 - a. On the Avaya Aura® Device Services web administration portal, navigate to **Service Connections > CORS Configuration > Admin Interface**.
 - b. From **SameSite cookie attribute value**, select **Strict**, **Lax**, or **None**.
 - c. Click **Save**.

Related links

[Configuring the SameSite attribute for web-based clients](#) on page 322

[Cross-origin resource sharing](#) on page 41

[Enabling Cross-origin resource sharing for the Service Interface](#) on page 41

[Enabling Cross-origin resource sharing for the Administrator Interface](#) on page 42

Configuring the SameSite attribute for web-based clients

About this task

If you use web-based clients, such as Avaya Workplace Client for web, in your deployment, you must set the SameSite attribute to **Lax**.

Procedure

1. On the Avaya Aura® Device Services web administration portal, go to **Service Connections > CORS Configuration > Service Interface**.
2. From **SameSite cookie attribute value**, select **Lax**.
3. Click **Save**.
4. Go to **Service Connections > CORS Configuration > Admin Interface**.
5. From **SameSite cookie attribute value**, select **Lax**.
6. Click **Save**.

Related links

[Configuring the SameSite cookie attribute](#) on page 321

Characters supported for Avaya Aura® Device Services passwords

You can use the following characters for Avaya Aura® Device Services passwords:

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

These rules apply to all passwords that you enter manually to access Avaya Aura® Device Services resources and for Keystore passwords.

 Note:

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

Password policy for human-user accounts

Human-user accounts are accounts that require you to enter a password manually to access Avaya Aura® Device Services resources. To protect data and prevent unauthorized access to the system, Avaya Aura® Device Services provides default complexity rules for human-user accounts. Each password you create for human-user accounts must meet these requirements.

Avaya Aura® Device Services enforces the default complexity rules for the following human-user accounts:

- Onboard Open LDAP
- Keycloak administrator
- SSH administration access to Avaya Aura® Device Services CLI
- Keepalived authentication
- Utility Server administration web console
- Cassandra database administrator

If your organization requires a different password policy, you can modify the default complexity rules by using the **sys passwdrules** command.

 Note:

- Avaya Aura® Device Services does not enforce complexity rules for the following passwords because they are not configured on Avaya Aura® Device Services:
 - Avaya Aura® Device Services web administration portal password.
 - System Manager enrollment password.

- Avaya Aura® Device Services does not apply complexity rules for the Keystore password because it is not considered to be a human-user account.

Configuring password rules

About this task

You can modify the default password complexity policy for human-user accounts.

Procedure

1. Log in to Avaya Aura® Device Services using an SSH connection.
2. Run the `sys passwdrules` command with appropriate arguments.

Related links

[passwdrules command](#) on page 458

Avaya Aura® Device Services entry points

The following table shows accounts that you can use to access various Avaya Aura® Device Services resources.

Login name	Accessible resources	Password change method
SSH administration user	• Virtual machine resources. • Avaya Aura® Device Services web administration portal, if additional STIG hardening is disabled. • Utility Server web administration portal, if Utility Server is enabled on Avaya Aura® Device Services.	Using the <code>passwd</code> command in the Avaya Aura® Device Services CLI.
Keycloak administration user	Keycloak web administration portal, if OAuth2 is enabled on Avaya Aura® Device Services.	• Using the Keycloak web administration portal. • Using the Avaya Aura® Device Services configuration utility.
Onboard Open LDAP administration user	• Avaya Aura® Device Services web administration portal, if Onboard Open LDAP is enabled. • Resource discovery and other REST calls that are performed using LDAP users.	Using the <code>recover_openldap.sh</code> command.
Cassandra database administration user	CLI-based Cassandra database administration.	Using the Avaya Aura® Device Services configuration utility.

Login name	Accessible resources	Password change method
Keepalived account	In a cluster environment, this account is used for IP takeover and to ensure High Availability.	Using the Avaya Aura® Device Services configuration utility.

HTTP Proxy

From release 10.2.1.1, you can configure HTTP proxies from the Client ID Configuration page.

When HTTP proxies are configured, the Avaya Aura® Device Services use the HTTP proxy to dynamically discover the metadata about the OpenID Connect (OIDC) provider if the OIDC URL is not directly accessible.

Specify the proxy in the following format: **<PROXY_HOST>:<PROXY_PORT>**. Providing incorrect inputs reject the entry, and an error message is displayed on the Avaya Aura® Device Services administrator user interface.

However, if no proxy address is configured, the OIDC discovery uses the OIDC URL directly, without any HTTP proxy.

Chapter 16: 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**.

Avaya Aura® Device Services 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

Name	Description
Virtual IP	Displays the virtual IP address and FQDN if a virtual IP address is configured. This is used as a load balancer node.
Virtual IPV6	Displays the virtual IPV6 address if IPV6 support is enabled.
Virtual IP Master	Displays the virtual IP and FQDN of the master node if a virtual IP address is configured.
Virtual IP Backup	Displays the virtual IP and FQDN of the backup node if a virtual IP address is configured.
Seed Node IP	Displays the IP address and FQDN of the seed node of the cluster.
Seed Node IPV6	Displays the IPV6 address of the seed node of the cluster, if IPV6 support is enabled.

Name	Description
Virtual IP Utility Server	Displays the virtual IP address and FQDN of the Utility Server.
Virtual IPV6 Utility Server	Displays the virtual IPV6 address of the Utility Server if IPV6 support is enabled.

Checking the Avaya Aura® Device Services status from the CLI

About this task

You can check whether the services of a local Avaya Aura® Device Services node are active using the command line interface. If Avaya Aura® Device Services indicates that any service is inactive, then the node is not working as expected.

Procedure

1. Log in to the Avaya Aura® Device Services CLI using an SSH connection.
2. Type `svc aads status`.

Result

The system displays the current status of services of the Avaya Aura® Device Services node.

- If a service is active, its status is “Running”.
- If a service is currently inactive, its status is “Not running”. In this case, Avaya Aura® Device Services also displays additional status information:
 - “Inactive”: The service is turned off.
 - “Activating”: The service is starting or restarting.

The following is an example of the command output where all services are active:

```
[admin@aads ~]$ svc aads status
```

```
Status of Avaya Aura Device Services Application
```

```
AADSTomcat      Running      n/a         11818
AADSNginx       Running      n/a         10246
AADSCassandra   Running      n/a         8121
AADSPostgres    Running      n/a         8767
AADSKeepalived  Running      n/a         10322
httpd           Running      n/a         9750
slapd           Running      n/a         13376
keycloak        Running      n/a         23857
```

Checking the status of a remote Avaya Aura® Device Services node from the CLI

About this task

You can run a health check for a remote Avaya Aura® Device Services node using the command line interface.

When you perform a health check, Avaya Aura® Device Services only displays the HTTP status code for the selected node as follows:

- 200: All services on the node are active and the node is working as expected.
- 503: One or more services on the node are not running.

Starting from Release 10.1.1.1, Avaya Aura® Device Services supports the HTTPS protocol for health checks.

! Important:

If you deploy Avaya Aura® Device Services on Microsoft Azure, you *must* use HTTPS for health checks to comply with the platform security policies.

If you need detailed information about the status of each service, use the `svc aads status` command. For more information, see [Checking the Avaya Aura Device Services status from the CLI](#) on page 327.

Before you begin

To run health checks using HTTPS, enable support for the HTTPS protocol. For more information, see [Enabling or disabling HTTPS for health checks](#) on page 329.

Procedure

1. Log in to the Avaya Aura® Device Services CLI using an SSH connection.
2. Do one of the following:

- To run a health check using HTTP, run the following command:

```
curl -k -v http://<NODE IP>:8457/health
```

- To run a health check using HTTPS, run the following command:

```
curl -k -v https://<NODE IP>:8457/health
```

In these commands, <NODE IP> is the IP address of a remote node whose status you want to check.

Result

Avaya Aura® Device Services displays the current status of the remote node.

The following is an example of the command output:

```
[admin@msg-aads ~]$ curl -k -v http://192.0.2.136:8457/health
* About to connect() to 192.0.2.136 port 8457 (#0)
* Trying 192.0.2.136...
* Connected to 192.0.2.136 (192.0.2.136) port 8457 (#0)
```

```
> GET /health HTTP/1.1
> User-Agent: curl/7.29.0
> Host: 192.0.2.136:8457
> Accept: */*
>
< HTTP/1.1 200
< Date: Fri, 12 Feb 2021 17:30:31 GMT
< Content-Length: 0
< Connection: keep-alive
<
* Connection #0 to host 192.0.2.136 left intact
```

Enabling or disabling HTTPS for health checks

About this task

By default, you can run health checks for nodes only using HTTP. To enhance security, you can enable HTTPS support for health check operations.

Procedure

1. Log in to the Avaya Aura® Device Services CLI using an SSH connection.
2. Run the following command:

```
cdto misc
```

3. Do one of the following:

- To enable HTTPS support for health checks, run the following command:

```
sudo ./https_healthCheck.sh --enable
```

- To disable HTTPS support for health checks, run the following command:

```
sudo ./https_healthCheck.sh --disable
```

Viewing performance statistics

About this task

You can review various performance metrics and system health indicators, such as CPU or memory usage, on the Avaya Aura® Device Services web administration portal. You can review performance metrics for specific nodes from logs currently available on Avaya Aura® Device Services or from an external performance log file.

Note:

Avaya Aura® Device Services stores performance logs a maximum of 30 days. You can collect logs for the future use as described in [Downloading logs](#) on page 336. Performance logs

have the AADS_perf_CLF.log file name format and they are located in the /opt/Avaya/DeviceServices/<build_number>/logs directory. Each log file contains metrics for a specific day.

Procedure

1. On the Avaya Aura® Device Services portal, go to **System Information > Performance Metrics**.
2. View performance data for a node for a specific day as follows:
 - a. Select **Choose Performance log from node by date**.
 - b. In **Nodes**, select the required node.
 - c. In **Date**, select the required date.
3. View performance metrics from an external performance log file as follows:
 - a. Select **Choose Performance Log file**.
 - b. From **File**, select a log file
4. Click **Retrieve**.

Avaya Aura® Device Services displays performance metrics in the Performance Metrics area. By default, Avaya Aura® Device Services displays the Summary tab.

If Avaya Aura® Device Services does not contain performance logs for the selected date, it displays a warning message.

Retrieving logs from an external file might take several seconds depending on the log file size and network bandwidth.

5. In the Performance Metrics area, click the tab that contains performance metrics you want to review.

For more information about performance metrics, see [Performance charts](#) on page 330.

6. **(Optional)** If you review performance metrics for the current date, click **Refresh** to update the metrics.

Related links

[Performance charts](#) on page 330

Performance charts

The following table lists the performance charts that you can see on the Performance Metrics page.

Chart	Description
Summary	Displays smaller versions of all available charts.

Chart	Description
CPU Usage	Displays CPU information, such as CPUs load, time spent waiting for input or output operations, or time used by user space processes. For example, you can use this chart to monitor whether the system load average threshold is exceeded due to spikes.  Note: If the average CPU usage exceeds 95%, Avaya Aura® Device Services raises an alarm on System Manager or on other SNMP server configured in your deployment.
Memory	Displays detailed information about the primary memory, including information about cached memory, available memory, buffered memory, and free space.
Disk Usage	Displays information about the secondary memory, including information about used and unused disk space.
Response Time	Displays the system response time in milliseconds. When any request is sent to Avaya Aura® Device Services, the system records the response time and then displays the aggregated information in this chart.
Auto Configuration Service Requests	Displays statistics related to requests to the Automatic Configuration Service. The chart displays information about successfully applied settings, invalid queries, or failed queries. The “Auto Configuration Service Request” chart displays the number of requests per second, and the “Auto Configuration Service RequestHrs” displays the number of requests per hour.
Automatic Configuration Service RequestsHrs	
Web Deployment Service Requests	Displays statistics related to requests to the Web Deployment Service. This chart monitors appcast items, such as the number of client uploads, downloads, or deployments. The “Web Deployment Service” chart displays the number of requests per second, and the “Web Deployment ServiceHrs” displays the number of requests per hour.
Web Deployment Service RequestsHrs	
User Service Request	Displays statistics related to requests to the Users API, such as adding or deleting a user or getting user details. This chart also displays whether these requests were successful or failed. The “User Service” chart displays the number of requests per second, and the “User ServiceHrs” displays the number of requests per hour.
User Service RequestHrs	
Picture Service Request	Displays statistics related to requests to the Workspace profile picture API. The “Picture Service Request” chart displays the number of requests per second, and the “Picture Service RequestHrs” displays the number of requests per hour.
Picture Service RequestHrs	

Chart	Description
Contact Service Request	Displays statistics related to requests to the Workspace contacts API, including adding, deleting or updating a contact requests. The “Contact Service Request” chart displays the number of requests per second, and the “Contact Service RequestHrs” displays the number of requests per hour.
Contact Service RequestHrs	

Related links

[Viewing performance statistics](#) on page 329

Logs

Log management

Avaya Aura® Device Services stores the common log at `/opt/Avaya/DeviceServices/<version>/logs/AADS.log`.

If a log file exceeds the log size limit, Avaya Aura® Device Services creates a new log file and keeps the old file on the system. When the number of log files exceeds 20, Avaya Aura® Device Services deletes the oldest log file. Avaya Aura® Device Services encrypts all log files that contain private information if they are older than the configured retention period.

You can view additional messages at `/opt/Avaya/DeviceServices/<version>/tomcat/<version>/logs/catalina`. For example, these messages can include the logs generated during the start of Avaya Aura® Device Services.

Related links

[Configuring the data retention period](#) on page 303

Configuring remote logging

About this task

You can configure Avaya Aura® Device Services to copy OS audit log onto a remote logging server. When remote logging is enabled, Avaya Aura® Device Services writes OS audit log file onto both the local and remote servers at the same time.

To maximize data privacy and security, you can use Kerberos to transfer logs to a remote logging server over a secure connection. For authentication, Kerberos uses a keytab file, which contains pairs of Kerberos principals and encrypted keys. Kerberos Distribution Center (KDC) generates the keytab file.

Before you begin

- Set up a remote logging server. The exact configuration process depends on the server that you use to store log files. You can use a Linux or Unix server.

- For a secure connection between Avaya Aura® Device Services and your remote logging server, configure the KDC on the remote logging server. The exact configuration process depends on the server that you use to store log files.
- If you want to use Kerberos authentication, obtain the keytab file from the KDC and upload it to Avaya Aura® Device Services using any file transfer program. You can upload the keytab file to the `/home` directory.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:


```
sys seconfig --stig --remote_audit
```
3. When you see the `Remote logging active?` prompt, type `yes`.
4. When you see the `Remote server FQDN?` prompt, type the FQDN of the remote storage server.
You must enter the FQDN. IP addresses are not supported.
5. When you see the `Remote logging port?` prompt, type `60`.
This is the default logging port value.
6. When you see the `Remote logging enable krb5?` prompt, type one of the following:
 - `yes`, if you want to use Kerberos to encrypt log files that Avaya Aura® Device Services off-loads to the remote server.
 - `no`, if you want to use an unencrypted connection to send log files to the remote server.
7. When you see the `Remote logging krb5_key_file?` prompt, do one of the following:
 - If Avaya Aura® Device Services displays the existing keytab file, press `Enter`.
 - If Avaya Aura® Device Services does not display an existing keytab file, provide the full path to the keytab file that you uploaded on Avaya Aura® Device Services and then press `Enter`.

The following is an example of the keytab file location: `/home/krb5.keytab`.

Avaya Aura® Device Services checks the keytab file and copies it to the `/etc` directory.

Monitoring 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
```


Avaya Aura® Device Services displays the logs generated during run time.

Changing a logging level

About this task

The logging level that you select determines which system events Avaya Aura® Device Services includes in log files. Avaya support personnel can use these log files to troubleshoot. If the log files that you provide do not contain enough information, support personnel will ask you to select another logging level.

Unless you are asked to change the logging level, use the WARNING level for all logging categories.

After selecting a new logging level, you must wait until the issue reoccurs before sending updated logs to support personnel. When the issue is resolved, you *must* switch back to the recommended logging level.

Important:

Increasing logging details results in larger log files and might also decrease the system performance.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Log Management > Log Level**.
2. In the **Logger** field, select the category to set up the logging level:
 - Avaya Aura® Device Services Logs: Collects the logs that the Avaya Aura® Device Services server generates.
 - System Logs: Collects all the system logs, including Keycloak logs.
 - All Logs: Collects all server and system logs.
3. 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. Use the FINEST level only to reproduce a specific server scenario and review the log.

Warning:

The FINE and FINEST logging levels can affect performance of the system. The risk is especially high on systems with a large number of end users. Enable the FINE and FINEST levels only for a short period, for example for 10 to 15 minutes, to

capture a specific issue. Do not use these options if they are not required. Enable the FINEST level when the system is under minimum load.

4. Click **Save**.

In cluster deployments, Avaya Aura® Device Services applies changes to all nodes in the cluster.

Scheduling log collection

About this task

Certain log levels, such as FINEST, provide very detailed information about events on Avaya Aura® Device Services. However, enabling these log levels on a constant basis might negatively impact the Avaya Aura® Device Services performance. You can enable detailed logging temporarily for a specified time period. After the specified period expires, Avaya Aura® Device Services switches back to the original log level, which you configure in the Adjust Service Logging Level area.

Scheduled log collection cancels automatically if you change the original log level for any log category.

After enabling scheduled log collection for a log category, you cannot set up scheduled log collections for other log categories until the specified time period expires or you cancel scheduled log collection.

Procedure

1. On the Avaya Aura® Device Services web administration portal, go to **Log Management > Log Level**.
2. In the Log capture scheduling area, select a log category for which you want to enable scheduled log collection.
3. In the **Planned log level** field, select a log level that you want to enable on a temporary basis for the log category.
4. **(Optional)** If required, repeat steps 2 and 3 for other log categories.
5. In the **Schedule Start Time** field, select one of the following:
 - **Immediate**: To start collecting logs at the planned log level immediately.
 - **Specify Time**: To specify the date and time when you want to start collecting logs at the planned log level.
6. In the **Duration** field, select one of the following:
 - **Select Duration**: To specify the period during which Avaya Aura® Device Services collects logs at the planned log level.
 - **No Duration (Indefinite)**: To set the log level specified in the **Planned log level** field as the new default log level for the log category.

 Note:

When you select **No Duration (Indefinite)**, Avaya Aura® Device Services does not schedule log collection at the specified log level. Instead, Avaya Aura® Device Services sets up the new default log level for the log category starting from the time specified in the **Schedule Start Time** field.

7. Click **Schedule**.
8. In the confirmation window, click **Save**.

Result

Avaya Aura® Device Services saves the configuration and displays the schedule status on the page.

Related links

[Canceling scheduled log collection](#) on page 336

Canceling scheduled log collection

About this task

You can cancel scheduled log collection at any time. If you cancel scheduled log collection when it is in progress, Avaya Aura® Device Services switches back to the original log level immediately.

Scheduled log collection cancels automatically if you change the original log level for any log category in the Adjust Service Logging Level area.

Procedure

1. On the Avaya Aura® Device Services web administration portal, go to **Log Management > Log Level**.
2. In the Log capture scheduling section, click **Cancel Schedule**.
3. In the confirmation window, click **Save** and then click **OK**.

Related links

[Scheduling log collection](#) on page 335

Downloading logs

About this task

Use this procedure to download Avaya Aura® Device Services logs to your computer. Support personnel can use the log files you collect for troubleshooting purposes.

You can only collect and download logs for one node at a time. You cannot download logs for an entire cluster at once.

To protect personal data, Avaya Aura® Device Services supports log anonymization for the logs you download. If you choose to anonymize logs, Avaya Aura® Device Services replaces all private or sensitive information with asterisk (*) symbols. Log files on Avaya Aura® Device Services remain unchanged.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Log Management > Log Level**.
2. In the Collect Logs area, in **Number of rotated log files to collect (1–20)**, enter the number of logs you want to download.

This setting specifies the number of files from the log file history to include in the log collection. The range is 1 to 20. If you leave this field empty, Avaya Aura® Device Services collects all available logs.

3. To collect logs for a node, click **Collect** in the corresponding row.
4. Wait until Avaya Aura® Device Services collects the logs and then click **OK**.
5. To download the logs you collected for a node, click **Download**.
6. When Avaya Aura® Device Services prompts you to anonymize logs, do one of the following:

- Click **Yes** to anonymize logs.

The anonymization process might take several minutes depending on the number of logs and the size of log files.

- Click **No** to just decrypt and download log files unchanged.

Related links

[collectlogs](#) on page 445

[Logs collected using the collectlogs command are encrypted](#) on page 426

Alarms

You can configure Avaya Aura® Device Services to send its alarms to an SNMP server.

- If you use Avaya Aura® Device Services in an Avaya Aura® environment, this is normally System Manager. However, if required, you can configure and use a third-party SNMP server.
- If you use Avaya Aura® Device Services in an environment without Avaya Aura®, you must configure and use a third-party SNMP server.

If FIPS is enabled, only SNMPv3 profiles are supported.

For more information, see *Administering Avaya Aura® System Manager*.

You can also view alarm details in the `/opt/Avaya/DeviceServices/<version>/logs/AADS_alarm.log` file.

Related links

[System Manager does not show Avaya Aura Device Services alarms](#) on page 407

Alarms configuration for System Manager

You can configure Avaya Aura® Device Services to send its alarms to an SNMP server. If you use Avaya Aura® Device Services in an Avaya Aura® environment, this is normally System Manager.

You must set up serviceability agents to receive Avaya Aura® Device Services alarms in System Manager. To configure serviceability agents, set up an SNMPv3 user profile and an SNMP target profile. Then assign the SNMPv3 user profile to the SNMP target profile.

Configuration Checklist

No.	Task	Notes	✓
1	Setup an SNMPv3 user profile.	See Setting up an SNMPv3 user profile on page 338.	
2	Setup an SNMP target profile.	See Setting up an SNMP target profile on page 339.	
3	Assign the SNMPv3 user profile.	See Assigning the SNMPv3 user profile on page 339.	

Setting up an SNMPv3 user profile

About this task

An SNMPv3 user profile enables you to define privileges so serviceability agents can read and write data in SNMP Management Information Bases (MIBs).

Procedure

1. On the System Manager web console, navigate to **Services > Inventory > Manage Serviceability Agents > SNMPv3 User Profiles**.
2. In the User Details section, click **Edit**.
3. In the **User Name** field, type `initial`.
4. In the **Authentication Protocol** field, select **SHA**.
The **MD5** setting is not supported.
5. In the **Authentication Password** field, type the authentication password.
The default authentication password is `avaya123`.
6. In the **Confirm Authentication Password** field, confirm the password.
7. In the **Privacy Protocol** field, select **AES**.
8. In the **Privacy Password** field, type the privacy password.
The default privacy password is `avaya123`.
9. In the **Confirm Privacy Password** field, confirm the password.
10. In the **Privileges** field, select **Read/Write**.
11. Click **Commit**.

Setting up an SNMP target profile

About this task

An SNMP target profile contains settings for sending alarms from Avaya Aura® Device Services to System Manager.

Procedure

1. On the System Manager web console, navigate to **Services > Inventory > Manage Serviceability Agents > SNMP Target Profiles**.
2. On the Target Details tab, click **Edit**.
3. In the **Name** field, type the name of the profile.
4. In the **Description** field, type a description for the profile.
5. In the **IP Address** field, type the System Manager IP address.
6. In the **Port** field, type 10162.
7. In the **Notification Type** field, select **Trap**.
8. In the **Protocol** field, select **V3**.
9. Click **Commit**.

Assigning the SNMPv3 user profile

About this task

You must assign the SNMPv3 user profile to the target profile so System Manager can receive alarms from Avaya Aura® Device Services.

Before you begin

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

Set up an SNMPv3 user profile and an SNMP target profile.

Procedure

1. On the System Manager web console, navigate to **Services > Inventory > Manage Serviceability Agents > Serviceability Agents**.
2. Select the Avaya Aura® Device Services host name, and click **Manage Profiles**.
3. Click the **SNMP Target Profiles** tab.
4. In the Assignable Profiles section, click the SNMP target profile you created, and click **Assign**.
5. Click the **SNMPv3 User Profiles** tab.
6. In the Assignable Profiles section, select the SNMPv3 profile you created, and click **Assign**.
7. Click **Commit**.

Alarms configuration for a third-party SNMP server

You can configure Avaya Aura® Device Services to send its alarms to an SNMP server. If you use Avaya Aura® Device Services in an environment without Avaya Aura®, you must configure and use a third-party SNMP server.

Configuration Checklist

No.	Task	Notes	✓
1	Setup SNMPv3 on the third-party server.	See Setting up a third-party SNMPv3 server on page 340.	
2	Configure the Avaya Aura® Device Services server to send alarms to the third-party server.	See Configuring Avaya Aura Device Services to support a third-party SNMP server on page 341.	
3	Verify that the third-party server receives Avaya Aura® Device Services alarms.	See Verifying third-party SNMP server operation on page 341.	

Setting up a third-party SNMPv3 server

About this task

In order to send alarms to a third-part server, the following elements must be configured on that server:

- SNMPv3 server software such as SNMP Manager on Linux.
- An SNMP user account configured on the third-party server. A matching user is configured on the Avaya Aura® Device Services server.
- Firewall access to the SNMP server. The defaults for most SNMP server installations are port 161 (UDP and TCP) for SNMP client access and port 162 for SNMP traps (UDP and TCP).

Procedure

1. Using the documentation for the third-party server operating system and/or the SNMP server software, verify the installation of the SNMP server.
2. Check that the third-party server is accessible on the ports configured for SNMP.
3. Check that you have the details for the SNMP server configured on the third-party server for use by Avaya Aura® Device Services. The required details are:
 - The user name.
 - The user's authentication password.
 - The user's encryption password.
 - The encryption algorithm to use; AES or DES.
 - The IP address of the SNMP server.
 - The destination port for SNMP traps on the SNMP server.

Configuring Avaya Aura® Device Services to support a third-party SNMP server

About this task

This process:

- Creates an SNMP user on the Avaya Aura® Device Services to match the one configured on the third-party SNMP server.

Adds the third-party SNMP server as the destination for alarms from the Avaya Aura® Device Services server.

Before you begin

- Configure the third-party server for SNMPv3 and create an SNMP user on that server.

Procedure

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

2. Run the following command:

```
cdto misc
```

3. Run the following command:

```
sudo ./setSNMPTrapDestination.sh -u <username> -A <authentication password> -X <encryption password> -x <encryption algorithm> -i <destination address> -p <destination port>
```

where:

- *<username>* is replaced with the SNMP username.
- *<authentication password>* is the SNMP user's authentication password.
- *<encryption password>* is the SNMP user's encryption password.
- *<encryption algorithm>* is the encryption algorithm, either AES or DES.
- *<destination address>* is the IP address of the third-party server running SNMP manager.
- *<destination port>* is the IP port for SNMP traps on the third-party server.

For example:

```
sudo ./setSNMPTrapDestination.sh -u snmpadmin -A 12345678 -X 34567890 -x DES -i 10.133.32.69 -p 162
```

Verifying third-party SNMP server operation

About this task

This process sends a set of test alarms from the Avaya Aura® Device Services server. Use these to check that the alarms are shown by the third-party SNMP server.

Procedure

1. On the Avaya Aura® Device Services server, use the following commands to send a set of test alarms:

```
cdto bin
sudo ./snmpTest.sh 1
```

2. Check that the third-party SNMP server displays the test alarms.

Avaya Aura® Device Services alarms list

The following table shows alarms that Avaya Aura® Device Services can trigger. You can view these alarms on System Manager or on other SNMP server configured in your deployment.

*** Note:**

Alarms that refer to Avaya Aura® solution components, such as System Manager or Session Manager, are not applicable if you use to Avaya Aura® Device Services in an environment without Avaya Aura®.

Alarm description	Severity	Event code	SNMP OID
AADS Disk space usage is below critical threshold	critical	OP_AADS-00099	.1.3.6.1.4.1.6889.2.89.0.99
AADS Disk space usage has reached critical threshold	critical	OP_AADS-00098	.1.3.6.1.4.1.6889.2.89.0.98
AADS Disk space usage is below warning threshold	minor	OP_AADS-00097	.1.3.6.1.4.1.6889.2.89.0.97
AADS Disk space usage has reached warning threshold	minor	OP_AADS-00096	.1.3.6.1.4.1.6889.2.89.0.96
AADS Restore process is successful	major	OP_AADS-00095	.1.3.6.1.4.1.6889.2.89.0.95
AADS Restore process failed	major	OP_AADS-00094	.1.3.6.1.4.1.6889.2.89.0.94
AADS Backup process is successful	major	OP_AADS-00093	.1.3.6.1.4.1.6889.2.89.0.93
AADS Backup process failed	major	OP_AADS-00092	.1.3.6.1.4.1.6889.2.89.0.92
The associated SM is back up and successfully reachable	critical	OP_AADS-00091	.1.3.6.1.4.1.6889.2.89.0.91
The associated SM is down and hence not reachable for SMGR	critical	OP_AADS-00090	.1.3.6.1.4.1.6889.2.89.0.90
AADS Server Node Licenses Threshold cleared	minor	OP_AADS-00089	.1.3.6.1.4.1.6889.2.89.0.89

Alarm description	Severity	Event code	SNMP OID
AADS Server Node Licenses Threshold reached	minor	OP_AADS-00088	.1.3.6.1.4.1.6889.2.89.0.88
AADS Server Node Licenses Available	major	OP_AADS-00087	.1.3.6.1.4.1.6889.2.89.0.87
AADS Server Node Licenses Unavailable	major	OP_AADS-00086	.1.3.6.1.4.1.6889.2.89.0.86
DRS is up clearing the alarm	major	OP_AADS-00083	.1.3.6.1.4.1.6889.2.89.0.83
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	major	OP_AADS-00082	.1.3.6.1.4.1.6889.2.89.0.82
Successfully connected to Exchange EWS service using delegate account	major	OP_AADS-00081	.1.3.6.1.4.1.6889.2.89.0.81
Not able to connect Exchange EWS service using delegate account	major	OP_AADS-00080	.1.3.6.1.4.1.6889.2.89.0.80
Successfully connected to PPM Web service	major	OP_AADS-00079	.1.3.6.1.4.1.6889.2.89.0.79
Not able to connect to PPM Web service	major	OP_AADS-00078	.1.3.6.1.4.1.6889.2.89.0.78
AADS Node Certificate is valid	major	OP_AADS-00077	.1.3.6.1.4.1.6889.2.89.0.77
AADS Node Certificate is expiring, has expired, or cannot be read	major	OP_AADS-00076	.1.3.6.1.4.1.6889.2.89.0.76
Synchronized with time server	major	OP_AADS-00075	.1.3.6.1.4.1.6889.2.89.0.75
Synchronization with time server lost	major	OP_AADS-00074	.1.3.6.1.4.1.6889.2.89.0.74
AADS Media storage is below critical threshold	critical	OP_AADS-00073	.1.3.6.1.4.1.6889.2.89.0.73
AADS Media storage has exceeded critical threshold	critical	OP_AADS-00072	.1.3.6.1.4.1.6889.2.89.0.72
AADS Media storage is below warning threshold	minor	OP_AADS-00071	.1.3.6.1.4.1.6889.2.89.0.71
AADS Media storage has exceeded warning threshold	minor	OP_AADS-00070	.1.3.6.1.4.1.6889.2.89.0.70

Alarm description	Severity	Event code	SNMP OID
AADS Connection to System Manager LDAP server was restored	major	OP_AADS-00069	.1.3.6.1.4.1.6889.2.89.0.69
AADS Connection to System Manager LDAP server was lost	major	OP_AADS-00068	.1.3.6.1.4.1.6889.2.89.0.68
AADS Backup Node released Virtual IP back to Primary	major	OP_AADS-00067	.1.3.6.1.4.1.6889.2.89.0.67
AADS Backup Node acquired Virtual IP from Primary	major	OP_AADS-00066	.1.3.6.1.4.1.6889.2.89.0.66
AADS Connection to Remote Domain was restored	major	OP_AADS-00065	.1.3.6.1.4.1.6889.2.89.0.65
AADS Connection to Remote Domain was lost	major	OP_AADS-00064	.1.3.6.1.4.1.6889.2.89.0.64
AADS is not operating in License Restricted Mode	critical	OP_AADS-00063	.1.3.6.1.4.1.6889.2.89.0.63
AADS is operating in License Restricted Mode	critical	OP_AADS-00062	.1.3.6.1.4.1.6889.2.89.0.62
AADS is not operating in License Error Mode	major	OP_AADS-00061	.1.3.6.1.4.1.6889.2.89.0.61
AADS is operating in License Error Mode	major	OP_AADS-00060	.1.3.6.1.4.1.6889.2.89.0.60
AADS JBoss Backend Certificate is valid	major	OP_AADS-00057	.1.3.6.1.4.1.6889.2.89.0.57
AADS JBoss Backend Certificate is expiring, has expired, or cannot be read	major	OP_AADS-00056	.1.3.6.1.4.1.6889.2.89.0.56
AADS OAM Certificate is valid	major	OP_AADS-00055	.1.3.6.1.4.1.6889.2.89.0.55
AADS OAM Certificate is expiring, has expired, or cannot be read	major	OP_AADS-00054	.1.3.6.1.4.1.6889.2.89.0.54
AADS REST Certificate is valid	major	OP_AADS-00053	.1.3.6.1.4.1.6889.2.89.0.53
AADS REST Certificate is expiring, has expired, or cannot be read	major	OP_AADS-00052	.1.3.6.1.4.1.6889.2.89.0.52
AADS Web Service has passed internal testing	major	OP_AADS-00051	.1.3.6.1.4.1.6889.2.89.0.51

Alarm description	Severity	Event code	SNMP OID
AADS Web Service has failed internal testing	major	OP_AADS-00050	.1.3.6.1.4.1.6889.2.89.0.50
AADS HTTP or SIP error code count is below threshold within time period	major	OP_AADS-00049	.1.3.6.1.4.1.6889.2.89.0.49
AADS HTTP or SIP error code count has exceeded threshold within time period	major	OP_AADS-00048	.1.3.6.1.4.1.6889.2.89.0.48
AADS Database storage is below critical threshold	critical	OP_AADS-00047	.1.3.6.1.4.1.6889.2.89.0.47
AADS Database storage has exceeded critical threshold	critical	OP_AADS-00046	.1.3.6.1.4.1.6889.2.89.0.46
AADS Database storage is below warning threshold	minor	OP_AADS-00045	.1.3.6.1.4.1.6889.2.89.0.45
AADS Database storage has exceeded warning threshold	minor	OP_AADS-00044	.1.3.6.1.4.1.6889.2.89.0.44
AADS System memory is below threshold	major	OP_AADS-00043	.1.3.6.1.4.1.6889.2.89.0.43
AADS System memory is exceeding threshold	major	OP_AADS-00042	.1.3.6.1.4.1.6889.2.89.0.42
AADS System log level is no longer set to debug, which will improve performance	minor	OP_AADS-00041	.1.3.6.1.4.1.6889.2.89.0.41
AADS System log level is set to debug, which will degrade performance	minor	OP_AADS-00040	.1.3.6.1.4.1.6889.2.89.0.40
AADS System load average is below threshold	major	OP_AADS-00037	.1.3.6.1.4.1.6889.2.89.0.37
AADS System load average is exceeding threshold	major	OP_AADS-00036	.1.3.6.1.4.1.6889.2.89.0.36
AADS total created accounts is below maximum	major	OP_AADS-00035	.1.3.6.1.4.1.6889.2.89.0.35
AADS total created accounts has reached maximum	major	OP_AADS-00034	.1.3.6.1.4.1.6889.2.89.0.34
AADS number of concurrent sessions is below maximum threshold	major	OP_AADS-00033	.1.3.6.1.4.1.6889.2.89.0.33
AADS number of concurrent sessions is exceeding maximum threshold	major	OP_AADS-00032	.1.3.6.1.4.1.6889.2.89.0.32

Alarm description	Severity	Event code	SNMP OID
AADS rate of requests/ responses went below maximum threshold	major	OP_AADS-00031	.1.3.6.1.4.1.6889.2.89.0.31
AADS is exceeding the maximum rate of requests/ responses within time period	major	OP_AADS-00030	.1.3.6.1.4.1.6889.2.89.0.30
AADS Connection to Session Manager was restored	major	OP_AADS-00029	.1.3.6.1.4.1.6889.2.89.0.29
AADS Connection to Session Manager was lost	major	OP_AADS-00028	.1.3.6.1.4.1.6889.2.89.0.28
AADS Connection to its Media Store was restored	major	OP_AADS-00027	.1.3.6.1.4.1.6889.2.89.0.27
AADS Connection to its Media Store was lost	major	OP_AADS-00026	.1.3.6.1.4.1.6889.2.89.0.26
AADS Connection to its Data Store was restored	major	OP_AADS-00025	.1.3.6.1.4.1.6889.2.89.0.25
AADS Connection to its Data Store was lost	major	OP_AADS-00024	.1.3.6.1.4.1.6889.2.89.0.24
AADS Connection to LDAP/ Active Directory server was restored	major	OP_AADS-00021	.1.3.6.1.4.1.6889.2.89.0.21
AADS Connection to LDAP/ Active Directory server was lost	major	OP_AADS-00020	.1.3.6.1.4.1.6889.2.89.0.20
Clear alarm	minor	OP_AADS-00002	.1.3.6.1.4.1.6889.2.89.0.2
An AADS Core Component was restarted successfully	major	OP_AADS-00011	.1.3.6.1.4.1.6889.2.89.0.11
An AADS Core Component has stopped functioning	major	OP_AADS-00010	.1.3.6.1.4.1.6889.2.89.0.10
AADS Automatic System Backup Failed	minor	OP_AADS-00178	.1.3.6.1.4.1.6889.2.89.0.178
AADS Automatic System Backup is Successful	minor	OP_AADS-00179	.1.3.6.1.4.1.6889.2.89.0.179
Certificate will expire soon. Please see Audit logs for more details	major	OP_AADS-00180	.1.3.6.1.4.1.6889.2.89.0.180
Certificate expiry date has been upgraded. It is OK now	major	OP_AADS-00181	.1.3.6.1.4.1.6889.2.89.0.181
Certificate has expired. Please see Audit logs for more details	critical	OP_AADS-00182	.1.3.6.1.4.1.6889.2.89.0.182

Alarm description	Severity	Event code	SNMP OID
Certificate has been renewed. It is OK now	critical	OP_AADS-00183	.1.3.6.1.4.1.6889.2.89.0.183
AADS average CPU usage has exceeded the critical threshold	critical	OP_AADS-00184	.1.3.6.1.4.1.6889.2.89.0.184
AADS average CPU usage is below the critical threshold	critical	OP_AADS-00185	.1.3.6.1.4.1.6889.2.89.0.185
Minimum TLS version changed to TLSv1.3	minor/info	OP_AADS-00206	.1.3.6.1.4.1.6889.2.89.0.206
Minimum TLS version changed back to TLSv1.2	clear/info	OP_AADS-00207	.1.3.6.1.4.1.6889.2.89.0.207
The number of users deleted from LDAP since the last synchronization exceeded the specified limit	critical	OP_AADS-00208	.1.3.6.1.4.1.6889.2.89.0.208
The number of users deleted from LDAP since the last synchronization did not exceed the specified limit	clear/info	OP_AADS-00209	.1.3.6.1.4.1.6889.2.89.0.209
Test alarm	minor	OP_AADS-00001	.1.3.6.1.4.1.6889.2.89.0.1
Avaya Spaces alarms			
AADS Spaces connection lost	critical	OP_AADS-00172	.1.3.6.1.4.1.6889.2.89.0.172
AADS Spaces connection restored	critical	OP_AADS-00173	.1.3.6.1.4.1.6889.2.89.0.173
AADS Spaces certificate expired	critical	OP_AADS-00174	.1.3.6.1.4.1.6889.2.89.0.174
AADS Spaces certificate restored	critical	OP_AADS-00175	.1.3.6.1.4.1.6889.2.89.0.175
AADS Spaces Host unreachable	critical	OP_AADS-00176	.1.3.6.1.4.1.6889.2.89.0.176
AADS Spaces Host reachable and connected	critical	OP_AADS-00177	.1.3.6.1.4.1.6889.2.89.0.177
Certificate revocation alarms			
Spaces certificate revoked	critical	OP_AADS-00186	.1.3.6.1.4.1.6889.2.89.0.186
Spaces revoked certificate OK	info	OP_AADS-00187	.1.3.6.1.4.1.6889.2.89.0.187
Spaces certificate CRL DP not reachable	critical	OP_AADS-00188	.1.3.6.1.4.1.6889.2.89.0.188

Alarm description	Severity	Event code	SNMP OID
Spaces certificate CRL DP is reachable and Certificate is OK	info	OP_AADS-00189	.1.3.6.1.4.1.6889.2.89.0.189
iView certificate revoked	critical	OP_AADS-00190	.1.3.6.1.4.1.6889.2.89.0.190
iView revoked certificate OK now	info	OP_AADS-00191	.1.3.6.1.4.1.6889.2.89.0.191
iView certificate CRL DP not reachable	critical	OP_AADS-00192	.1.3.6.1.4.1.6889.2.89.0.192
iView certificate CRL DP is reachable and Certificate is OK	info	OP_AADS-00193	.1.3.6.1.4.1.6889.2.89.0.193
SM certificate revoked	critical	OP_AADS-00194	.1.3.6.1.4.1.6889.2.89.0.194
SM revoked certificate is OK	info	OP_AADS-00195	.1.3.6.1.4.1.6889.2.89.0.195
SM certificate CRL DP not reachable	critical	OP_AADS-00196	.1.3.6.1.4.1.6889.2.89.0.196
SM certificate CRL DP is reachable and certificate is OK	info	OP_AADS-00197	.1.3.6.1.4.1.6889.2.89.0.197
SMGR certificate revoked	critical	OP_AADS-00198	.1.3.6.1.4.1.6889.2.89.0.198
SMGR revoked certificate is OK	info	OP_AADS-00199	.1.3.6.1.4.1.6889.2.89.0.199
SMGR Certificate CRL DP not reachable	critical	OP_AADS-00200	.1.3.6.1.4.1.6889.2.89.0.200
SMGR certificate CRL DP is reachable and certificate is OK	info	OP_AADS-00201	.1.3.6.1.4.1.6889.2.89.0.201
LDAP certificate revoked.	critical	OP_AADS-00202	.1.3.6.1.4.1.6889.2.89.0.202
LDAP revoked certificate OK now	info	OP_AADS-00203	.1.3.6.1.4.1.6889.2.89.0.203
LDAP certificate CRL DP not reachable	critical	OP_AADS-00204	.1.3.6.1.4.1.6889.2.89.0.204
LDAP certificate CRL DP is reachable and Certificate is OK	info	OP_AADS-00205	.1.3.6.1.4.1.6889.2.89.0.205
Minimum TLS version changed to TLSv1.3	minor/info	OP_AADS-00206	.1.3.6.1.4.1.6889.2.89.0.206
Minimum TLS version changed back to TLSv1.2	clear/info	OP_AADS-00207	.1.3.6.1.4.1.6889.2.89.0.207

Enhanced Access Security Gateway for real time support

Enabling the Enhanced Access Security Gateway from the CLI

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.

Procedure

1. Open the SSH console as an administrator.
2. Run the following command to check the EASG status:

```
EASGStatus
```

By default, the EASG status is disabled.

3. Run the following command to enable EASG:

```
sudo /usr/sbin/EASGManage --enableEASG
```

4. Run the following command to verify the product certificate:

```
sudo EASGProductCert --certInfo
```

Avaya Aura® Device Services displays the product certificate details.

For example:


```
[admin@amm-ova-test ~]$ EASGStatus
EASG is disabled
[admin@amm-ova-test ~]$ 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 - 12:28
[admin@amm-ova-test ~]$ 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=
                  .O, OU=EASG, O=Avaya Inc.
[admin@amm-ova-test ~]$
```

If the certificate expires within 360, 180, 30, or 0 days, Avaya Aura® Device Services writes a certificate expiry notification to the `/var/log/messages` log 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 17: 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. Avaya Aura® Device Services creates automatic backups on a weekly basis, and you can create manual backups when required. The backup and restore procedures are the same, regardless of the deployment method.

Important:

If you change the IP addresses or FQDN of an Avaya Aura® Device Services node, you *cannot* use backups created before you made these changes to restore the data. This limitation applies to both manual and automatic backups.

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.

Backing 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:

- Avaya recommends that you start a Tmux session before running the backup command. If the SSH session terminates while the backup operation is in progress, you can re-connect to the Tmux session and complete the backup operation. For more information about the Tmux utility, see [Using the Tmux utility](#) on page 466.
- 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 258.

Procedure

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

2. To start a Tmux session, run the following command:

```
tmux new-session -s <NAME>
```

In this command, `NAME` is a Tmux session name of your choice. For example:

```
tmux new-session -s AADS_backup_session
```

3. To create a backup, run one of the following commands:

- `app backup -t` To create a backup in a `.tar.zip` file.
- `app backup` To create a backup in a directory.

4. If you created your backup in a `.tar.zip` file, provide a password when prompted and then re-enter the password to confirm.

If the password does not comply with the password complexity rules, Avaya Aura® Device Services prompts you to enter a new password. For more information about the password complexity rules, see [passwdrules command](#) on page 458.

5. 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.

6. Ensure that the administrator's home directory contains the backup file or backup directory.
7. Copy the backup files to an external storage using a file transfer program, such as SFTP or SCP.
8. In a cluster environment, repeat steps 6 and 7 on all remaining nodes in the cluster.
9. To retrieve the casandra username and password, refer to [Retrieving Cassandra database username and password](#) on page 355.
10. To locate the keystore password, refer to [Locating keystore password](#) on page 355.

Automatic backups

Avaya Aura® Device Services creates backups of configuration files and user data automatically on a weekly basis. Avaya Aura® Device Services uses the following default settings for automatic backups:

Setting	Value
Date and time	Each Sunday at 12:00 a.m.
Backup file location	<code>/var/log/Avaya/backup/</code>
Number of backups stored	Three rotating backups
Password	<code>RAPtor@WELcomE</code>

If required, you can update the default automatic backup settings using the Avaya Aura® Device Services web administration portal.

 Important:

- Avaya Aura® Device Services recommends that you change the default password for automatic backups immediately after installing or upgrading Avaya Aura® Device Services.
- If STIG hardening is enabled, for automatic backups, you must configure a password 15-character long or more. The default password does not meet STIG requirements and will cause backup failure. You can review the current password rules using the **sys passwdrules show** command.
- In cluster deployments, if any Avaya Aura® Device Services node is down, then the automatic backup creation process fails.

If the backup creation process fails, Avaya Aura® Device Services generates an alarm on System Manager or on other SNMP server configured in your deployment.

 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 258.

Configuring automatic backups

About this task

Use this procedure to modify the default automatic backup settings. By default, Avaya Aura® Device Services starts creating automatic backups each Sunday at 12:00 a.m.

The backup process requires significant system resources. Therefore, schedule automatic backups during the least busy periods to minimize the impact on Avaya Aura® Device Services performance.

 Important:

Avaya Aura® Device Services recommends that you change the default password.

Procedure

1. Log in to the Avaya Aura® Device Services web administration portal.
2. Go to **Backup Settings > Automatic Backup Configuration**.
3. In **Backup Time**, specify the time and date to start creating automatic backups.
4. Select the **Repeat every** check box and then specify the time interval between two consecutive automatic backup operations.
5. In **Max Backup**, specify how many backups you want to store on Avaya Aura® Device Services.
6. Change the password that is currently used for automatic backups as follows:
 - a. Select the **Change Password** check box.

- b. In **Backup File Password**, type a password of your choice for backups.

The password must comply with the password complexity rules. You can view the rules by pointing the cursor to the **Backup File Password** field.

 Important:

If STIG hardening is enabled, you must configure a password of 15 characters or more.

- c. In **Re-Enter Password**, type the password again.

7. Click **Save**.

Related links

[passwdrules command](#) on page 458

Changing the location of automatic backups

About this task

By default, Avaya Aura® Device Services stores automatic backups in the `/var/log/Avaya/backup/` directory. You can change the location of backup files by modifying the `tomcat.start.sh` file. You cannot change the location from the Avaya Aura® Device Services web administration portal.

Existing automatic backup files remain in the location where they were created. Avaya Aura® Device Services does not move these files to the new location.

 Note:

- Avaya recommends that you use the default location for automatic backups.
- After the Avaya Aura® Device Services upgrade, the location of automatic backups is changed back to the default location. You must repeat this procedure if you want to store automatic backups in another directory.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator using an SSH connection.
2. Open the `tomcat.start.sh` file in the vi text editor with sudo privileges:

```
sudo vi /opt/Avaya/DeviceServices/<version>/CAS/<version>/service.d/
tomcat.start.sh
```

3. In the `CATALINA_OPTS="$CATALINA_OPTS -Dcom.avaya.cas.autobackup.dir=<DIRECTORY_NAME>"` string, replace the existing `<DIRECTORY_NAME>` entry with the path to the directory where you want to store automatic backups.

For example, if you want to store automatic backups in the `home/admin/automatic_backups/` directory, modify the string as follows:

```
CATALINA_OPTS="$CATALINA_OPTS -Dcom.avaya.cas.autobackup.dir=/home/
admin/automatic_backups/"
```

4. Save the file.
5. Run the following command to restart Tomcat:

```
svc tomcat restart
```

Retrieving Cassandra database username and password

About this task

Before restoring Avaya Aura® Device Services application, you must retrieve the Cassandra username and password.

Procedure

1. Navigate to Cassandra database:

```
cdto cas
```
2. Access the binary folder:

```
cd bin
```
3. To retrieve the Cassandra username, run the following command:

```
sudo ./getDBCreds.sh DB_USER
```
4. To retrieve the Cassandra password, run the following command:

```
sudo ./getDBCreds.sh DB_PASSWORD
```

Locating keystore password

Procedure

1. Navigate to the utilities directory:

```
cdto misc
```
2. Locate the Java truststore password:

```
sudo ./crypt.sh getProperty ../config/keystores.properties  
JAVA_TRUSTSTORE_PASSWORD
```
3. Locate the tomcat JMX password:

```
sudo ./crypt.sh getProperty ../config/cas-settings.properties  
tomcatJmxPassword
```

Avaya Aura® Device Services configuration portability

You can export the configuration data of an Avaya Aura® Device Services node to a `.properties` file. You can use the exported data to facilitate the Avaya Aura® Device Services installation process in migration or reinstall scenarios. The exported file contains all the parameters required for silent installation, and most of the parameters are already properly configured. Therefore, you can install Avaya Aura® Device Services in silent mode using this file instead of manually configuring the required settings during the interactive installation.

Configuration file structure

The exported `.properties` file contains the set of parameters in the following format:

```
<PARAMETER_NAME>=<PARAMETER VALUE>
```

For example:

```
INCLUDE_OPENLDAP=n  
CASSANDRA_VER=  
INCLUDE_OAUTH=n  
USE_LDAP_FOR_AUTH=y  
KEYSTORE_PW=<>
```

Most of the parameters required for silent installation contain the required values. For the parameters, such as `KEYSTORE_PW`, where values are set to “<>”, you must provide values relevant to the server where you install Avaya Aura® Device Services. You do not need to modify parameters that have no value set, such as `REST_FRONTEND_HOST`.

Limitations

The exported configuration file only supports silent installation. You cannot use this file for interactive installations.

Use case example

The following is a simplified example of an Avaya Aura® Device Services node restoration using the exported configuration file:

1. Redeploy virtual machines.
2. In the exported configuration file, modify the parameters where values are set to “<>” according to your deployment settings.
3. Reinstall the Avaya Aura® Device Services application in silent mode using the exported configuration file.
4. Restore configuration and user data from backup files.

Exporting the configuration file using the web administration portal

About this task

Use this procedure to collect configuration data from an Avaya Aura® Device Services node using the web administration portal.

Before you begin

In cluster deployments, if you plan to export the configuration file for another node, ensure that RSA keys are configured for SSH connections in the cluster. For more information, see “Configuring RSA public and private keys for SSH connections in a cluster” in *Deploying Avaya Aura® Device Services*.

Procedure

1. On the Avaya Aura® Device Services web administration portal, go to **Service Control > Application Management**.
2. In the Export Application Configuration area, click **Download** for the appropriate node.

Result

Avaya Aura® Device Services collects configuration data for the node and exports the file to your computer. The exported file name has the `_export.<NODE_IP_ADDRESS>-<DATE>-<TIME>.properties` format.

Exporting the configuration file using the CLI

About this task

Use this procedure to collect configuration data from an Avaya Aura® Device Services node using the CLI.

Before you begin

In cluster deployments, if you plan to export the configuration file for another node, ensure that RSA keys are configured for SSH connections in the cluster. For more information, see “Configuring RSA public and private keys for SSH connections in a cluster” in *Deploying Avaya Aura® Device Services*.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator using an SSH connection.
2. Run the following command:


```
cdto misc
```
3. Do one of the following:
 - To generate a configuration file for the current node, run the following command with `sudo` privileges:


```
sudo ./exportConfigForSilentInstall.sh generate
```
 - To generate a configuration file for another node in a cluster, run the following command:


```
sudo ./exportConfigForSilentInstall.sh generate -ip
<NODE_IP_ADDRESS>
```

Avaya Aura® Device Services generates the configuration file and displays the full path to the file.

4. **(Optional)** Download the file to your computer using a file transfer utility of your choice, such as SFTP, SCP, or WinSCP.

Preparing the exported configuration file for silent installation

About this task

Before using the exported configuration file for silent installation, you must provide valid values for parameters whose values equal to "<>".

You do not need to modify parameters that have no value set.

Before you begin

Ensure that you have a configuration file for an appropriate Avaya Aura® Device Services node.

Procedure

1. Open the configuration file in a text editor of your choice.
2. For each parameter whose value equals to "<>", provide a value appropriate for your deployment.
3. Save the file.

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.

Note:

Avaya recommends that you restore Avaya Aura® Device Services in a Tmux session. If the SSH session terminates while the restoration operation is in progress, you can re-connect to the Tmux session and complete the restoration operation. For more information about the Tmux utility, see [Using the Tmux utility](#) on page 466.

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.
- If you changed the IP address or FQDN of the node, ensure that the required Avaya Aura® Device Services backup was created after these changes. You *cannot* restore the node using backups created before you changed the node IP address or FQDN.
- 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. If you use Avaya Aura® Device Services in an Avaya Aura® environment, 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. If you use Avaya Aura® Device Services in an Avaya Aura® environment, 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 you use third-party identity certificates, in the **Front-end host, System Manager and Certificate Configuration** menu, configure the following options to provide the paths to the certificate and key files:
 - REST interface key file
 - REST interface certificate file
 - OAM interface key file
 - OAM interface certificate file

- node key file
 - node certificate file
 - signing authority certificate file
- h. 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. If you use Avaya Aura® Device Services in an Avaya Aura® environment, on System Manager, verify that DRS replication is working.
- For more information, see [Checking for DRS synchronization](#) on page 393.
3. On the Avaya Aura® Device Services web administration portal, force LDAP synchronization and ensure that Avaya Aura® Device Services does not display the 503 Service Unavailable error.
- For more information, see [Setting up user synchronization with the LDAP server](#) on page 202.
4. Copy the backup file or backup directory to the home directory of the administrative user using a file transfer utility, such as SFTP or SCP.
5. To start a Tmux session, run the following command:

```
tmux new-session -s <NAME>
```

In this command, <NAME> is a Tmux session name of your choice. For example:

```
tmux new-session -s AADS_RESTORE
```

6. To restore the backed-up configuration files, run the following command:

```
app restore <path>
```

In this command, <path> is the absolute path to the backup file in .tar.zip format or to the backup directory.

7. When prompted, enter the password you used to create the backup.

If the password is wrong, Avaya Aura® Device Services prompts you to re-enter the password. After three failed attempts, Avaya Aura® Device Services aborts the restore process. In this case, you will need to run the `app restore` command again.

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 259.

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 previous backup.

*** Note:**

Avaya recommends that you restore Avaya Aura® Device Services in a Tmux session. If the SSH session terminates while the restoration operation is in progress, you can re-connect to the Tmux session and complete the restoration operation. For more information about the Tmux utility, see [Using the Tmux utility](#) on page 466.

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 or backup directory. When restoring an Avaya Aura® Device Services node, you must use the correct backup file or directory for that node.
- If you changed IP addresses or FQDNs of Avaya Aura® Device Services nodes, ensure that the required Avaya Aura® Device Services backup files were created after these changes. You *cannot* restore a node using backup files created before you changed the IP address or FQDN of the 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. If you use Avaya Aura® Device Services in an Avaya Aura® environment, 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. If you use Avaya Aura® Device Services in an Avaya Aura® environment, 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 use third-party identity certificates, in the **Front-end host, System Manager and Certificate Configuration** menu, configure the following options to provide the paths to the certificate and key files:
 - REST interface key file
 - REST interface certificate file
 - OAM interface key file
 - OAM interface certificate file
 - node key file
 - node certificate file
 - signing authority certificate file
 - j. If you enabled the Utility Server, configure the settings in the **Clustering Configuration** menu.
 - k. 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. On the seed node, configure SSH/RSA public and private keys.

For more information, see “Configuring RSA public and private keys for SSH connections in a cluster” in *Deploying Avaya Aura® Device Services*.
 3. If OAuth was enabled on the system that you are restoring, enable OAuth database replication on all nodes in the cluster.

For more information, see [Enabling OAuth database replication in a cluster environment](#) on page 151.

4. If onboard Open LDAP was enabled on the system that you are restoring, enable Open LDAP replication on all nodes in the cluster.

For more information, see [Enabling Open LDAP replication](#) on page 391.

5. If you use Avaya Aura® Device Services in an Avaya Aura® environment, on System Manager, verify that DRS replication is working for all nodes.

For more information, see [Checking for DRS synchronization](#) on page 393.

6. On the Avaya Aura® Device Services web administration portal, force LDAP synchronization and ensure that Avaya Aura® Device Services does not display the 503 Service Unavailable error.

Perform this step on each node in the cluster.

For more information, see [Setting up user synchronization with the LDAP server](#) on page 202.

Perform steps 1 to 4 on the seed node first and then on all non-seed nodes.

7. Copy the backup file or backup directory 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 or backup directory created for the current node.

8. To start a Tmux session, run the following command:

```
tmux new-session -s <NAME>
```

In this command, <NAME> is a Tmux session name of your choice. For example:

```
tmux new-session -s AADS_RESTORE
```

9. To restore the backed-up configuration files, run the following command:

```
app restore <path>
```

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

10. When prompted, enter the password you used to create the backup.

If the password is wrong, Avaya Aura® Device Services prompts you to re-enter the password. After three failed attempts, Avaya Aura® Device Services aborts the restore process. In this case, you will need to run the `app restore` command again.

11. Repeat steps [7](#) on page 363 to [10](#) on page 363 on the non-seed nodes.

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

```
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 259.

Synchronizing client ID

About this task

After Avaya Aura® Device Services is restored, if the Keyloak is enabled, the public key for the client ID resets to default value.

Before you begin

- Restore Avaya Aura® Device Services.
- Restore the existing configuration details for Avaya Aura® Device Services. For more information, refer to [Restoring an Avaya Aura Device Services cluster](#) on page 360.

Procedure

1. Navigate to **Security Settings > Client ID Mapping**.
2. Under **Client to Identify Provider Mapping**, click **Sync** for the required client ID.

Chapter 18: Avaya Aura® Device Services upgrade and migration operations

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

Upgrade or migration path number	From	To
1	8.0.2	8.1.3
2	8.1.3	8.1.4
3	8.1.4	8.1.5
4	8.1.5	10.1.0
5	10.1.0	10.1.1
6	10.1.1	10.1.1.1
7	10.1.x	10.2.x

Depending on the release you are currently using, you might need to perform several upgrade or migration procedures. For example, to upgrade Avaya Aura® Device Services Release 8.1.5 to Release 10.1.1.1, follow paths 4, 5, and 6.

This document focuses on the upgrade process for path 7. For information about migration and upgrade processes for previous releases, see the following documents:

- Avaya Aura® Device Services Release 8.1.3 and Release 8.0.2 use different operating system versions. Therefore, you cannot upgrade from Release 8.0.2 to 8.1.3. You must perform a migration as described in the referenced chapter. This requirement applies to all deployment types.
- For Release 8.1.4, see [Avaya Aura® Device Services upgrade and migration operations](#).
- For Release 8.1.5, see [Avaya Aura® Device Services upgrade and migration operations](#).
- For Release 10.1.0, see [Avaya Aura® Device Services upgrade and migration operations](#)

Avaya Aura® Device Services Release 10.1.0 and Release 8.1.5 use different operating system versions. Therefore, you cannot upgrade from Release 8.1.5 to 10.1.0. You must perform a migration as described in the referenced chapter. This requirement applies to all deployment types.

- For Release 10.1.1, see the chapter “Avaya Aura® Device Services upgrade and migration operations” in [Administering Avaya Aura® Device Services](#).

! Important:

- Perform the system layer update before upgrading Avaya Aura® Device Services.
- Avaya Aura® Device Services does not support rollback with the migration process.
- Starting from Release 10.1.1, you can deploy Avaya Aura® Device Services in an environment without Avaya Aura®. In this mode, Avaya Aura® Device Services does not require Avaya Aura® components, such as System Manager or Session Manager, to operate. However, you cannot select this option when upgrading from Release 10.1.0 to 10.1.1. After upgrading to Release 10.1.1, Avaya Aura® Device Services continues to operate in an Avaya Aura® environment. To use Avaya Aura® Device Services in an environment without Avaya Aura®, you must fresh install Avaya Aura® Device Services.

Avaya Aura® Device Services upgrade checklist

Perform the tasks in this checklist to upgrade Avaya Aura® Device Services to Release 10.2.x.

This checklist applies AWS and ESXi OVA-based deployments and to software-only deployments. For AVP OVA-based deployments, see the upgrade procedures in [Upgrading Avaya Aura Device Services on AVP](#) on page 377.

No.	Task	Description	✓
1	Back up Avaya Aura® Device Services.	See Backing up Avaya Aura Device Services on page 351.	
2	Update the system layer, if required.	• For OVA-based deployments, see the procedures in Checklist for updating the system layer on page 368. • For software-only deployments, see Updating the system layer for software-only deployments on page 371. In a cluster environment, update the system layer on all cluster nodes before upgrading the application layer.	
3	Upgrade the application layer.	For upgrade steps, see Upgrading Avaya Aura Device Services on page 372.	

Avaya Solutions Platform migration considerations

Avaya Solutions Platform 120

Avaya Aura® Device Services Release 10.1.0 does not support Avaya Solutions Platform 120. Therefore, you must upgrade your Avaya Solutions Platform 120 to Avaya Solutions Platform 130 Release 5 before migrating to Avaya Aura® Device Services Release 10.1.0.

Note:

Avaya Solutions Platform 120 is synonymous with Avaya Converged Platform 120 and Appliance Virtualization Platform (AVP).

Avaya Solutions Platform 130

Avaya Solutions Platform 130 Release 4 uses the ESXi hypervisor version that Avaya Aura® Device Services Release 10.1.0 does not support. Therefore, if you use Avaya Solutions Platform 130 Release 4, you must upgrade it to Avaya Solutions Platform 130 Release 5 before migrating to Avaya Aura® Device Services Release 10.1.0. For more information about upgrading Avaya Solutions Platform, see [Upgrading Avaya Solutions Platform from Release 4.0 to 5.0](#) on page 367.

Upgrading Avaya Solutions Platform from Release 4.0 to 5.0

About this task

Use the following procedure to upgrade the Avaya Solutions Platform from Release 4.0 (ESXi 6.5, Update3) to Release 5.0 (ESXi 7.0, Update2).

Procedure

1. Take the backup of your Avaya Aura® Device Services and keep it on remote servers.
2. Log in to the application through vSphere Web Client, select and right-click the Avaya Aura® Device Services application, and then click **Power** > **Power Off**.
3. Upgrade Avaya Solutions Platform from Release 4.0 to 5.0.

For information about upgrading Avaya Solutions Platform from Release 4.0 to 5.0, see “Avaya Solutions Platform 130 Series: Upgrading to ESXi 7.0 u2 from ESXi 6.5.x”.

If the Avaya Solutions Platform upgrade is successful, power on the Avaya Aura® Device Services application and ensure the applications are up and running.

If the Avaya Solutions Platform upgrade failed, then:

- Do the fresh deployment of Avaya Solutions Platform 130 Release 5.0. For information about installing Avaya Solutions Platform, see “Installing the Avaya Solutions Platform 130 Series”.
 - Deploy the application at the same version that was before the Avaya Solutions Platform upgrade. For information about deploying the application, see the application-specific deployment document.
4. If the Avaya Aura® Device Services applications are not up and running:
 - a. Do the fresh deployment of the application at the same version that was before the Avaya Solutions Platform upgrade.

- b. Restore the backup taken at step 1.

System layer (operating system) updates for virtual machines deployed using Avaya-provided OVAs

Each virtual machine that is created by deploying the Avaya Aura® Device Services OVA file has a system layer (operating system). The system layer 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 applies to virtual machines deployed in a VMware virtual environments using Avaya-provided OVAs. For information about updating the system layer in software-only deployments, see [Updating the system layer for software-only deployments](#) on page 371.

Checklist for updating the system layer

Use this checklist to update the system layer. This checklist applies to OVA-based deployments.

No.	Task	Notes	
1	Determine if the system layer update is applicable to the given virtual machine.	See Determining if a system update is applicable on page 368. Skip the remaining steps if the update is not applicable.	
2	Download, extract, and stage the update.	See Downloading, extracting, and staging a system layer update on page 369.	
3	Install the update during a maintenance window.	See Installing a staged system layer update on page 370.	

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. The virtual machine might be 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:

Ignore the patch level reported by the above command.

Next steps

- If the above system version is already on the recommended system update, then no further action is required.
- If the 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 website, 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 the installation of the update.

 Tip:

Avaya recommends cleaning 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.

Procedure

1. Download the update from the [Avaya Support](#) website.
`ucapp-system-3.4.3.0.7.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, run the following command:

```
tar -zxvf ucapp-system-<version>.tgz
```

For example:

```
tar -zxvf ucapp-system-3.4.3.0.7.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-3.4.3.0.7
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-3.4.3.0.7.tgz
rm -rf ucapp-system-3.4.3.0.7
```

7. To verify that the update has been staged, query the status:

```
sysUpdate --status
```

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.

8. **(Optional)** If a system update is staged in error, run the following command to delete this staged update:

```
sysUpdate --delete
```

You cannot delete a staged update once the installation of the update has started.

9. **(Optional)** For more information about the **sysUpdate** command, run one of the following commands:

```
sysUpdate --help
sysUpdate --hhelp
```

The **--help** option provides the command line syntax. The **--hhelp** option provides verbose help.

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, you can install it. 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.
Avaya Aura® Device Services reboots after the installation process completes.
3. **(Optional)** Run one of the following commands to monitor the progress of the update:

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

The `--monitor` option uses the Linux tail browser. The `--monitor less` option uses the Linux less browser.

4. **(Optional)** Run the following command to review the status of the update:

```
sysUpdate --status
```

5. **(Optional)** Run the following command to obtain logs of the current and previous system layer update installations:

```
sysUpdate --logs
```

This command gathers log files into an archive in ZIP format and places this archive in the current working directory.

Next steps

If your organization requires stricter STIG compliance, re-enable additional STIG hardening after you finish installing the system layer update. For more information, see [Enabling additional STIG hardening](#) on page 317.

Updating the system layer for software-only deployments

About this task

The system layer is low-level software that provides the required operational environment for the Avaya Aura® Device Services application. You must update the system layer before upgrading your Avaya Aura® Device Services application.

For software-only deployments, Avaya provides a system layer installer in a package, which also contains an Avaya Aura® Device Services application installer.

For information about installing system layer updates for OVA-based deployments, see [System layer \(operating system\) updates for virtual machines deployed using Avaya-provided OVAs](#) on page 368.

Before you begin

Download the latest `aads-swonly-<AADS_VERSION>.tgz` software-only installation package from PLDS.

Procedure

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

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

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

```
tar -xzf aads-swonly-<AADS_VERSION>.tgz
```

For example: `tar -xzf aads-swonly-10.1.1.0.x.tgz`

The `/root/aads-swonly-AADS_RELEASE/` directory contains the following files:

- The system layer package in TGZ archive `ucapp-swonly-system-<VERSION>.tgz`.
- The Avaya Aura® Device Services application binary `aads-<AADS_RELEASE>.bin`.

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

```
cd aads-swonly-<AADS_VERSION>
```

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

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

For example: `tar - xzf ucapp-swonly-system-1.0.0.0.8.tgz`

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

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

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

```
./swOnlyUpdate.sh --patch
```

Upgrading Avaya Aura® Device Services

About this task

This procedure provides the high-level steps for upgrading Avaya Aura® Device Services to Release 10.2.x.

This procedure applies to the following deployment types:

- OVA-based deployments on an ESXi host.
- All software-only deployments.

If you have Avaya Aura® Device Services deployed on a on an Appliance Virtualization Platform (AVP) host, see the upgrade procedures in [Upgrading Avaya Aura Device Services on AVP](#) on page 377.

This procedure also describes cluster deployments. If you have a standalone Avaya Aura® Device Services deployment, ignore the references to other cluster nodes.

*** 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 either [System layer \(operating system\) updates for virtual machines deployed using Avaya-provided OVAs](#) on page 368 or [Updating the system layer for software-only deployments](#) on page 371 depending on your deployment type.

2. Perform a full system backup.

These backups are used if you need to abort the upgrade procedure and roll back to the currently installed Release 10.1.1.x.

3. Upgrade the virtual machines:
 - a. Upgrade the system layer.
 - b. Upgrade the Avaya Aura® Device Services application.

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 10.2.x.

Procedure

Complete [Backing up Avaya Aura Device Services](#) on page 351.

Next steps

Upgrade ESXi and AWS virtual machines.

Upgrading the Avaya Aura® Device Services application

About this task

Use this procedure to upgrade the Avaya Aura® Device Services application layers on the existing virtual machines.

*** Note:**

Avaya recommends that you upgrade Avaya Aura® Device Services in a Tmux session. If the SSH session terminates while the upgrade operation is in progress, you can re-connect to the Tmux session and complete the upgrade operation. For more information about the Tmux utility, see [Using the Tmux utility](#) on page 466.

Before you begin

- Back up your Avaya Aura® Device Services Release 10.1.1.x system.
- Download the system layer update file and the latest binary installer file.
- Upgrade to the latest system layer release on all nodes.

! 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

In a cluster environment, perform steps [1](#) on page 374 to [12](#) on page 375 on the seed node first, then on the backup node, and then on all other non-seed nodes in the cluster.

1. Log in to a node as an administrator using an SSH connection.
2. To start a Tmux session, run the following command:

```
tmux new-session -s <NAME>
```

In this command, <NAME> is a Tmux session name of your choice. For example:

```
tmux new-session -s AADS_UPGRADE
```

3. **(Optional)** To enable IPv6 support for ESXi deployments, run the following command to enable IPv6 at the system layer:

```
sys ipv6config set
```

+ Tip:

For general information about the `sys ipv6config` command, run the following command:

```
sys ipv6config -h
```

! Important:

AWS deployments *do not* support IPv6.

4. Run the following command to remove the inactive Avaya Aura® Device Services version:

```
app removeinactive
```

5. Transfer the binary file to the administrator home folder on Avaya Aura® Device Services by using a file transfer tool of your choice.
6. Run the following command to make the file executable:

```
chmod 755 aads-<version>.bin
```

For example:

```
chmod 755 aads-10.1.1.0.16.bin
```

7. Run the following command to start the upgrade:

```
app upgrade aads-<version>.bin
```

For example:

```
app upgrade aads-10.1.1.0.16.bin
```

8. 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 disable it on all nodes. You cannot enable the Utility Server on some cluster nodes and disable it on other nodes.

9. When the system prompts you to enable onboard Open LDAP, do one of the following:

- If you want to enable onboard Open LDAP, select **Yes**.
- If you do not want to enable onboard Open LDAP, select **No**.

 Note:

If you enable onboard Open LDAP when upgrading, you will not be able to roll back to the previously installed release.

10. When the system prompts you to enable OAuth, do one of the following:

- If want to enable OAuth, select **Yes**.
- If you do not want to enable OAuth, select **No**.

11. **(Optional)** When the system prompts you to enable IPv6, do the following:

- If you want to enable IPv6, select **Yes** and then provide virtual IPv6 addresses of your choice for Avaya Aura® Device Services and the Utility Server, if it is enabled.
- If you do not want to enable IPv6, select **No**.

This step is only applicable if you enabled IPv6 at the system layer in step [3](#) on page 374.

12. Follow the system prompts to complete the upgrade procedure.
13. In a cluster environment, repeat the steps above on the backup node and then on all other non-seed cluster nodes.
14. If you enabled OAuth, on the seed node, configure Keycloak settings as described in “Configuring Keycloak settings” in *Deploying Avaya Aura® Device Services*.
15. If you enabled IPv6, on all nodes, configure the virtual IPv6 address and Utility Server virtual IPv6 address using the Avaya Aura® Device Services configuration utility.
16. If you use onboard Open LDAP, enable Open LDAP replication on all nodes in the cluster.

For more information, see [Enabling Open LDAP replication](#) on page 391.

17. Log in to the seed node as an administrative user using an SSH connection.
18. Run the `svc aads restart` command to restart Avaya Aura® Device Services.
19. In a cluster environment, repeat steps [17](#) on page 376 and [18](#) on page 376 on all other cluster nodes.
20. If you use Avaya Aura® Device Services in an Avaya Aura® environment, verify that DRS replication is working for all nodes on System Manager.

For more information, see [Checking for DRS synchronization](#) on page 393.

21. From the seed node, run the following commands to generate personal information metadata:

```
cdto misc
sudo ./clearPhoneNumberLastSync.sh
```

22. From the Avaya Aura® Device Services web administration portal, perform synchronization with LDAP.

For more information, see [Setting up user synchronization with the LDAP server](#) on page 202.

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 388.
- If you want to use Advanced Intrusion Detection Environment (AIDE), create a baseline database as described in [AIDE tool management](#) on page 311.

Rolling back the 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.

Note:

Avaya recommends that you roll back Avaya Aura® Device Services in a Tmux session. If the SSH session terminates while the rollback operation is in progress, you can re-connect to the Tmux session and complete the rollback operation. For more information about the Tmux utility, see [Using the Tmux utility](#) on page 466.

Important:

- You *cannot* roll back to the previously installed release if you enabled and configured onboard Open LDAP when upgrading to the current release.
- If you perform a rollback after changing Avaya Aura® Device Services IP addresses or FQDNs, Avaya Aura® Device Services will continue using these new IP addresses or FQDNs after the rollback. The rollback process does not revert IP address or FQDN changes.

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.

Before you begin

Complete [Upgrading the Avaya Aura Device Services application](#) on page 373.

Procedure

1. Using an SSH connection, log in as an administrator to the node that you last upgraded.
2. To start a Tmux session, run the following command:

```
tmux new-session -s <NAME>
```

In this command, <NAME> is a Tmux session name of your choice. For example:

```
tmux new-session -s AADS_ROLLBACK
```

3. Run the following commands to perform the rollback for this node:

```
cd
app rollback
```

4. 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.

5. Log in to the seed node as an administrator using an SSH connection.
6. Run the `svc aads start` command to start Avaya Aura® Device Services.
7. Repeat steps [5](#) on page 377 to [6](#) on page 377 for the backup node first and then for all other non-seed nodes.

Next steps

If SSO/OAuth was enabled on the system that you are restoring, enable OAuth replication on all nodes in the cluster. For more information, see “Enabling OAuth database replication in a cluster environment” in *Deploying Avaya Aura® Device Services*.

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 10.2.x 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 10.2 OVA to create new virtual machines for each node in the cluster.

4. Restore the Avaya Aura® Device Services Release 10.2.x application using the backups created in step [2](#) on page 378.

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](#) on page 378.
 - c. Restore the cluster.

! Important:

You *cannot* rollback to Release 10.1.1.x if you enabled disk encryption when deploying Release 10.2 OVAs in step [3](#) on page 378.

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 10.2.x.

Procedure

1. Record the currently installed version of the Avaya Aura® Device Services application.
To upgrade to Release , you must have Avaya Aura® Device Services Release 10.1.1.x.
2. Back up the cluster as described in [Backing up Avaya Aura Device Services](#) on page 351.
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 379.

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.

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 -nr | 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](#) on page 380 to [9](#) on page 381 for all remaining nodes in the cluster.

Next steps

Upgrade the existing AVP virtual machines.

Upgrading the Avaya Aura® Device Services application on AVP virtual machines

About this task

Use this procedure to upgrade the Avaya Aura® Device Services 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 10.2 OVAs.

* Note:

Avaya recommends that you upgrade Avaya Aura® Device Services in a Tmux session. If the SSH session terminates while the upgrade operation is in progress, you can re-connect to the Tmux session and complete the upgrade operation. For more information about the Tmux utility, see [Using the Tmux utility](#) on page 466.

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 379.
- 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 \(operating system\) updates for virtual machines deployed using Avaya-provided OVAs](#) on page 368.

! 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

In a cluster environment, repeat steps [1](#) on page 381 to [12](#) on page 383 on the seed node first, then on the backup node, and then on all other non-seed nodes in the cluster.

1. Log in to a node as an administrator using an SSH connection.
2. To start a Tmux session, run the following command:

```
tmux new-session -s <NAME>
```


In this command, <NAME> is a Tmux session name of your choice. For example:

```
tmux new-session -s AADS_UPGRADE
```

3. **(Optional)** To enable IPv6 support, run the following command to enable IPv6 at the system layer:

```
sys ipv6config set
```

+ Tip:

For general information about the `sys ipv6config` command, run the following command:

```
sys ipv6config -h
```

4. Run the following command to remove the inactive Avaya Aura® Device Services version:

```
app removeinactive
```

5. 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.

6. Run the following command to make the file executable:

```
chmod 755 aads-<version>.bin
```

For example:

```
chmod 755 aads-8.1.5.0.16.bin
```

7. Run the following command to start the upgrade:

```
app upgrade aads-<version>.bin
```

For example:

```
app upgrade aads-8.1.5.0.16.bin
```

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

9. When the system prompts you to enable onboard Open LDAP, do one of the following:

- If you want to enable onboard Open LDAP, select **Yes**.
- If you do not want to enable onboard Open LDAP, select **No**.

10. When the system prompts you to enable OAuth, do one of the following:

- If you want to enable OAuth, select **Yes**.
- If you do not want to enable OAuth, select **No**.

11. **(Optional)** When the system prompts you to enable IPv6, do the following:
 - If you want to enable IPv6, select **Yes** and then provide virtual IPv6 addresses of your choice for Avaya Aura® Device Services and the Utility Server, if it is enabled.
 - If you do not want to enable IPv6, select **No**.

This step is only applicable if you enabled IPv6 at the system layer in step [3](#) on page 382.

12. Follow the system prompts to complete the upgrade procedure.
13. Repeat the steps above on the backup node first, and then on all other non-seed nodes in the cluster.
14. If you enabled OAuth, on the seed node, configure Keycloak settings as described in “Configuring Keycloak settings” in *Deploying Avaya Aura® Device Services*.
15. If you enabled IPv6, on all nodes, configure the virtual IPv6 address and Utility Server virtual IPv6 address using the Avaya Aura® Device Services configuration utility.
16. If onboard Open LDAP was enabled on the system that you are restoring, enable Open LDAP replication on all nodes in the cluster.

For more information, see [Enabling Open LDAP replication](#) on page 391.

17. Log in to the seed node as an administrative user using an SSH connection.
18. Run the `svc aads start` command to start Avaya Aura® Device Services.
19. Repeat steps [17](#) on page 383 and [18](#) on page 383 on all other cluster nodes.
20. Verify that DRS replication is working for all nodes on System Manager.

For more information, see [Checking for DRS synchronization](#) on page 393.

21. Log in to the seed node as an administrative user using an SSH connection.
22. 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.

23. Transfer the backup file to an off-board storage location using a file transfer program, such as SFTP or SCP.
24. Repeat steps [23](#) on page 383 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 10.2.x virtual machines to complete the upgrade. To improve efficiency, you can perform multiple 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 10.1.1.x 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 10.2 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 379.
 - d. Attach the new virtual machine to the network recorded for the node in [Preparing for an AVP upgrade](#) on page 379.
 - 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, copy the installer to the administrative user's home directory using a file transfer program, such as SFTP or SCP.
7. Repeat the previous step for all other cluster nodes.

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 10.2.x.

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 Avaya Aura Device Services application on AVP virtual machines](#) on page 381 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 360.

4. Verify that DRS replication is working for all nodes on System Manager.

For more information, see [Checking for DRS synchronization](#) on page 393.

5. From the seed node, run the following commands to generate personal information metadata:

```
cdto misc
sudo ./clearPhoneNumberLastSync.sh
```

6. From the Avaya Aura® Device Services web administration portal, perform synchronization with LDAP.

For more information, see [Setting up user synchronization with the LDAP server](#) on page 202.

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 388.
- Configure AIDE scanning and ClamAV antivirus security tools as described in [Security options](#) on page 311.

Rolling back the AVP upgrade

About this task

Use this procedure to abort the upgrade procedure and roll back from Avaya Aura® Device Services Release 10.2.x to Release 10.1.1.x.

Important:

Rollback is *not* supported if you enabled disk encryption when you deployed new Release 10.2 OVA's.

Based on the state of the system at the time when you decided to roll back, 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 379.
- 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 10.2.x 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 10.2.x virtual machine and turn off the power:

```
sudo shutdown -hP now
```

4. Repeat the steps [1](#) on page 386 to [3](#) on page 386 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.
 - c. Configure the new server with the server configuration information you saved from the node while performing [Preparing for an AVP upgrade](#) on page 379.
 - 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 379.

- e. Repeat substeps [5.a](#) on page 386 to [5.d](#) on page 386 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, copy the installer to the administrative user's home directory using a file transfer program, such as SFTP or SCP.
 7. Repeat step [6](#) on page 386 for all other cluster nodes:
 8. On the Home page of the System Manager web console, navigate to **Elements > Session Manager > System Status > User Data Storage**.
 9. Click **Backup and Restore**.
 10. Select the Session Manager on which you want to run the restore operation.
 11. Click **Restore**.
 12. From the "Restore File" column, select the backup that you created while performing [Preparing for an AVP upgrade](#) on page 379.

13. Do one of the following:
 - Click **Commit** to accept the selection.
 - Click **Reset** to reload the Restore File selection list.
 - Click **Cancel** to cancel the restore request and return to the User Data Storage screen.
14. 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**.
15. Restore the Avaya Aura® Device Services cluster as described in [Restoring an Avaya Aura Device Services cluster](#) on page 360.

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

About this task

After nodes are added to a cluster, you must configure the RSA public and private keys to enable internode SSH communications.

Use this procedure to configure the RSA public and private keys on the initial node for the entire cluster.

Before you begin

Install all of the required nodes for the cluster.

Procedure

1. Log in to the Linux shell on the initial Avaya Aura® Device Services node as an administrator.
2. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.
3. Navigate to **Clustering Configuration > Cluster Utilities > Configure SSH RSA Public/Private Keys**.
Avaya Aura® Device Services displays the RSA Public and Private key configuration tool.
4. When the system displays the `Add additional hosts to the list? (y/n)` prompt, enter `y` (yes) if you are generating keys for the first time or if you need to generate keys for a new node in the cluster.
Otherwise, enter `n` (no).
5. If you chose to update the node list in the previous step, when Avaya Aura® Device Services prompts you, enter the IP address of the non-seed node in the cluster you want to generate keys for and then press `Enter`.

6. Repeat the previous step for all remaining non-seed nodes.
7. When Avaya Aura® Device Services prompts you to enter a user name for a node, enter the username for the Linux administrator account that you used to perform the Avaya Aura® Device Services installation.
8. If Avaya Aura® Device Services prompts you to replace the existing keys, enter `y` (yes).
9. When Avaya Aura® Device Services prompts you to enter a password, enter the password for the Linux administrator account that you used to perform the installation.
10. When the configuration is complete, press `Enter`.
11. Return to the main menu.
12. From the main menu, select **Continue** and then select **Yes** to apply the changes.

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://<IP_address>:8543/admin.html`

In this URL, <IP_address> is the IP address of an Avaya Aura® Device Services node.

 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 **Choose file** 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:

```
cdto misc
sudo ./clitool-acs.sh upgradeAutoConfigTestConfigurations
```

This command automatically upgrades the existing test configurations.

Running a patch to allow Avaya Workplace Client for Windows to connect to the Web Deployment service

About this task

For software updates through Avaya Workplace Client 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 if you have Avaya Workplace Client for Windows clients and ESG servers in your environment.

If you have only Avaya Aura® Device Services and Avaya Workplace Client 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 Workplace Client for Windows to reach the Web Deployment service.
- **disable:** To revert the workaround to allow Avaya Workplace Client 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. Run the following command:

```
cdto misc
```

2. Run the following command:

```
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/<nginx version>/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 the 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.

For example, `https://<AADS FQDN or IP Address>:8442/acs/resources/webdeployment/downloads/Avaya Equinox Setup 3.0.0.136.msi`.

6. Change the APPCAST URL port in Dynamic Configurations to 8442.

For example, `https://<AADS FQDN or 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:

```
cdto misc
sudo ./dynamicconfigurations-patch.sh enable
```

Enabling Open LDAP replication

About this task

Enable Open LDAP database replication in a cluster deployment. This procedure is not applicable for standalone installations.

Before you begin

- Ensure that an FQDN is assigned to each node in the cluster.
- Ensure that each node is accessible from all other nodes in the cluster.
- From a node CLI, run the `app listnodes` command and ensure that all cluster nodes have the “live” status.

Procedure

1. Run the Avaya Aura® Device Services configuration utility using the `app configure` command.

2. Select **Enable Open LDAP Replication**.
3. Select **Enable Open LDAP Replication** again.
4. Select **Yes**.
5. Select **Open LDAP Password**. and enter the Open LDAP administrator password.
6. Select **OK**.

The data replication process might take several minutes to complete.

7. After the data replication is complete, select **Continue**.
8. To ensure that data replication is enabled, view the `/var/log/Avaya/openldap/openldap.log` file.

The following is an example of a `/var/log/Avaya/openldap/openldap.log` file entry indicating that data replication is enabled:

```
Jan 21 11:11:11 aads1 slapd[23992]: conn=1015 fd=17 ACCEPT from IP=1.2.3.5:63930
(IP=1.2.3.4:3268)
Jan 21 11:11:11 aads1 slapd[23992]: conn=1015 op=0 BIND
dn="cn=administrator,dc=company,dc=com" method=12
Jan 21 11:11:11 aads1 slapd[23992]: conn=1015 op=0 BIND
dn="cn=administrator,dc=company,dc=com" mech=SIMPLE ssf=0
Jan 21 11:11:11 aads1 slapd[23992]: conn=1015 op=0 RESULT tag=97 err=0 text=
```

If `/var/log/Avaya/openldap/openldap.log` contains error messages, such as `ldap_sasl_bind_s failed rc -1`, then some nodes are not accessible. In this case, you must make these nodes accessible from other nodes and then repeat the data replication procedure.

9. Repeat steps 1 to 8 on all remaining nodes on the cluster.

Re-enabling Open LDAP replication after removing a node from a cluster

About this task

Removing a node from a cluster affects Open LDAP replication. After a node is removed from the cluster, you must re-enable Open LDAP replication manually.

Important:

When you perform this procedure, *all* LDAP user data will be erased. After the procedure is complete, you must re-upload the user data using the Avaya Aura® Device Services web administration portal.

Before you begin

Ensure that you have a copy of the user data currently stored in Open LDAP.

Procedure

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

2. Run the following commands:

```
cdto openldap
sudo ./recover_openldap.sh
```

! Important:

This script erases *all* user data stored in Open LDAP.

3. Repeat steps 1 to 2 on all remaining nodes in the cluster.
4. On each cluster node, perform the Open LDAP replication procedure.

Checking for DRS synchronization

About this task

The DRS process synchronizes data between System Manager and Avaya Aura® Device Services. The synchronization time varies depending on the network and number of users in the system. Services might fail if DRS is not in sync. Therefore, ensure that DRS is synchronized after installation.

This procedure is not required if you deploy Avaya Aura® Device Services in an environment without Avaya Aura®.

Procedure

1. In System Manager, go to **Services > Replication**.
2. Select the replication group.
3. Search for the Avaya Aura® Device Services nodes and check whether they are listed as Synchronized.

The following is an example of a synchronized Avaya Aura® Device Services system.

Replica Nodes				
View Details Repair Remove Remove From Queue Show All Replica Groups				
1 Item				
☐	Replica Node Host Name	Product	Synchronization Status	Last Synchronization Time
☐	aads164.apac.avaya.com	AADS	Synchronized	December 27, 2019 2:28:10 PM +05:30
Select : All, None				

Setting up user synchronization with LDAP after deployment

About this task

Before using Avaya Aura® Device Services, you must synchronize the user with the LDAP server.

Procedure

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

Avaya Aura® Device Services displays the Enterprise LDAP Server Configuration page.

3. In the User Synchronization Update Instructions section, do the following:

- a. Click **Force LDAP Sync**.

Avaya Aura® Device Services displays the following message:

```
WARNING!Force LDAP Sync will re-synchronize all the LDAP
user data. This action will impact on-going Device Services
operations and must be performed during a maintenance window.
```

- b. Click **OK**.

Avaya Aura® Device Services displays the following message:

```
Starting update.
```

- c. Click **OK**.

- d. Ensure that Avaya Aura® Device Services displays the following message:

```
Last Sync Status : Successful as on : <date and time of the
synchronization>.
```

```
For example: Last Sync Status : Successful as on : Tue, Sep 06,
2016 13:54:36 (UTC+5:30) .
```

- e. Specify a date and time to schedule the synchronization of Avaya Aura® Device Services users with the Enterprise LDAP Server users.
- f. Select the **Repeat** check box and click the day to set up a recurring event for synchronization.
- g. Click **Save**.

Chapter 19: Upgrading RHEL 8.4 to RHEL 8.10 on OVA- based virtual machines

About this task

You can upgrade RHEL 8.4 to RHEL 8.10 using the following **av-upgrade-os** command. The **av-upgrade-os** command is available when Avaya Aura® Device Services R10.2.1 is installed.

Before you begin

1. Install Avaya Aura® Device Services R10.2.1.

To view the current version of Avaya Aura® Device Services, run the following command:
svc aads swversion.

2. Verify that **av-upgrade-os** command is available.

To verify if the **av-upgrade-os** command is available, run the following command: **which av-upgrade-os**

3. Verify the current version of RHEL on which Avaya Aura® Device Services is running.

To view the current RHEL version, run any of the following commands:

- **cat /etc/redhat-release**
- **av-version**

4. Download Avaya Aura® Device Services RHEL 8.10 Operating System bundle on Avaya Aura® Device Services R10.2.1 virtual machine.

Procedure

1. Login to Avaya Aura® Device Services CLI.
2. To upgrade from RHEL 8.4 to RHEL 8.10, run the following command: **av-upgrade-os <AADS RHEL OS Bundle>**

For example, run **av-upgrade-os AV-AADS10.2-RHEL8.10-OSUpdate-001.tar.bz2**

3. After successful upgrade to RHEL 8.10, reboot the Avaya Aura® Device Services virtual machine.
4. Login to Avaya Aura® Device Services CLI.

5. To verify that RHEL 8.10 is upgraded successfully, run any of the following commands:

- **cat /etc/redhat-release**
- **av-version**

Chapter 20: Troubleshooting

Avaya Workspaces Client cannot connect to Avaya Aura[®] Device Services

Condition

Avaya Workspaces Client is unable to connect to Avaya Aura[®] Device Services.

The browser displays the following error:

For example,

```
Your connection is not private
Attackers might be trying to steal your information from aads.xyz.avaya.com (for
example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
Subject: aads.xyz.avaya.com
Issuer: System Manager CA
Expires on: Nov 14, 2024
Current date: Jul 31, 2023
PEM encoded chain:-----BEGIN CERTIFICATE-----
MIIEvTCCA6WgAwIBAgIULIWE+z6Rgvi68M5o99kcxpm0avMwDQYJKoZIhvcNAQEL
BQAwOzEaMBGGA1UEAwRU3lzdGVtIE1hbmFnZXIgaQ00ExDTALBgNVBAsMBE1HTVQx
```

The browser console logs displays the following error:

For example,

```
GET https://aads.xyz.avaya.com/abc/resources net::ERR_CERT_AUTHORITY_INVALID
GET https://aads.xyz.avaya.com/abc/resources net::ERR_CERT_AUTHORITY_INVALID
```

Cause

Avaya Aura[®] Device Services is using ID certificates issued by System Manager/ Private/ Third-party CA and this CA certificate is not available out of the box for the browser and it does not trust the System Manager/ Private/ Third-party CA.

Solution

Install Enterprise CA certificate.

For example, System Manager/ Private/ Third-party CA's on the user's machine, where the user is accessing Workspaces in the browser. So that the browser can trust System Manager/ Private/ Third-party CA certificate and can access the Avaya Aura[®] Device Services APIs for search.

Troubleshooting for the DRS service

The DRS troubleshooting procedures in this section are applicable for Avaya Aura® Device Services deployed in an Avaya Aura® environment.

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

[Changing a logging level](#) on page 334

[Checking for DRS synchronization](#) on page 393

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. Log in to the Avaya Aura® Device Services CLI as the root user.
 - b. Go to the `/opt/Avaya/DeviceServices/<build>/CAS/<build>/drs` directory.
 - c. Run the following commands in sequence:

```
removeReplicationEntry.sh
drsInstall.sh
drsStart.sh
```

Avaya Aura® Device Services installation or upgrade fails due to invalid System Manager certificates

Condition

In an Avaya Aura® environment, Avaya Aura® Device Services installation or upgrade fails due to invalid System Manager certificates.

Cause

During the installation or upgrade process, Avaya Aura® Device Services connects to System Manager to obtain certificates required for installation. If the System Manager certificates contain unsupported critical extensions, expired, or the certificate start date is in the future, Avaya Aura® Device Services does not import these certificates and stops the installation or upgrade process.

Solution

Contact the System Manager administrator.

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 contains 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.jav
a:57)
at
com.avaya.cas.datastore.ConfigurationStore.getServerConfigParamFromRow(ConfigurationStor
e.java:2164)
at
com.avaya.cas.datastore.ConfigurationStore.getAllServerConfigurations(ConfigurationStore
.java:2062)
at
com.avaya.acs.cli.AadsCryptoToolCliApp.encryptLdapPasswords(AadsCryptoToolCliApp.java:17
0)
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.

Admin user is not prompted for password in sudo su

Solution

The "90-cloud-init-users" file in /etc/sudoers.d/ gets created by cloud-init and adds the following rule for admin user:

For example, for an admin or administrative user, cloud-init adds the rule `admin ALL=(ALL) NOPASSWD:ALL`.

This file has limited permission. Even the "root" user has read-only access.

To overcome this problem, move "90-cloud-init-users" file to user's home dir.

For example, `mv /etc/sudoers.d/90-cloud-init-users /home/admin/`

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 Workplace Client for Windows and Avaya Workplace Client for Mac must be moved to another web server or to the Avaya Aura® Device Services web server on a unchallenged web port.

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, Avaya Aura® Device Services cannot create the `/authorized_keys` file. The log file displays a disk space warning.

Solution

Clean up the `/home` directory.

DNS entries disappear from the `/etc/resolv.conf` file after restarting Avaya Aura® Device Services

Condition

DNS entries disappear from the `/etc/resolv.conf` after restarting Avaya Aura® Device Services.

Cause

The NetworkManager service controls the content of the `/etc/resolv.conf` file. This service automatically changes the content of the file to the “default” state when Avaya Aura® Device Services is restarted.

Solution

1. Open the `/etc/NetworkManager/NetworkManager.conf` file in a text editor.

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

2. Navigate to the `[main]` section in the file and do one of the following:

- If the `[main]` section contains an entry starting with `dns`, replace this entry with the `dns=none` entry.
- If the `[main]` section does not contain an entry starting with `dns`, add the `dns=none` entry to the `[main]` section.

For example:

```
[main]
dns=none
```

3. Save the file.
4. Run the following command to restart the NetworkManager service:

```
systemctl restart NetworkManager
```

Check for Updates feature is not working

Condition

The Check for Updates feature on Avaya Workplace Client for Windows does not work and an error is displayed.

Solution

1. On the Windows computer where Avaya Workplace 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. Close Avaya Workplace 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 Avaya Workplace Client.
5. If the Check for Updates feature is still not working, go to **Client Settings > Support**.
6. Click **Reset Application**.
7. Configure Avaya Workplace 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.

Primary System Manager fails

Condition

The primary System Manager fails. Geographic redundancy is enabled in System Manager.

Cause

Avaya Aura® Device Services does not support the System Manager geographic redundancy mode. Therefore, Avaya Aura® Device Services cannot switch to the secondary System Manager automatically.

Solution

If the primary System Manager fails and you need to use Avaya Aura® Device Services before it is restored, perform the following steps to enroll Avaya Aura® Device Services against the secondary System Manager. In a cluster environment, perform these steps on each cluster node.

Important:

After the primary System Manager is back online, you must re-enroll against the primary System Manager.

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the `app configure` command.
3. Select **Front-end host, System Manager and Certificate Configuration**.
4. Select **System Manager FQDN** and provide the FQDN of the secondary System Manager.
5. Select **System Manager Enrollment Password** and provide the enrollment password of the secondary System Manager.
6. Click **Apply**.
7. When the primary System Manager is back online, repeat this procedure and provide the FQDN and the enrollment password of the primary System Manager.

Cannot connect to System Manager after replacing a revoked System Manager certificate with a valid certificate

Condition

If a System Manager certificate that is used to connect to Avaya Aura® Device Services is revoked, Avaya Aura® Device Services stops connecting to System Manager. However, Avaya Aura® Device Services does not re-connect to System Manager even when the revoked System Manager certificate is replaced with a valid certificate.

This issue is not applicable if Avaya Aura® Device Services is deployed in an environment without Avaya Aura®.

Cause

Avaya Aura® Device Services does not re-connect to System Manager automatically after revoked certificates are replaced on System Manager. You must re-connect Avaya Aura® Device Services to System Manager manually.

Solution

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
In a cluster deployment, log in to the seed node.
2. Run the following commands to disable certificate revocation checks:

```
cdto misc
./clitool-acs.sh resetCertificateRevocationCheckToDefault
```
3. Run the following commands:

```
cdto misc
./blockunblocksmgr.sh unblock
```
4. In a cluster deployment, repeat the previous step on all cluster nodes.
5. Re-configure the certificate revocation audit policy as appropriate.

For more information see [Configuring the revocation check policy](#) on page 235.

Related links

[Certificate revocation management](#) on page 233

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.

This issue is not applicable if Avaya Aura® Device Services is deployed in an environment without Avaya Aura®.

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..`

4. Restart Avaya Aura® Device Services.

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 dataIntegrityAuditDiagnostics 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 05 Oct 2020 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/
8.5.57/lib/log4j.properties: java.io.FileNotFoundException: /opt/Avaya/DeviceServices/
7.1.2.0.557/CAS/7.1.2.0.557/tomcat/8.5.57/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

Alarms are generated on Avaya Aura® Device Services, and user profiles are appropriately created and assigned, but System Manager does not show these alarms.

This issue is not applicable if Avaya Aura® Device Services is deployed in an environment without Avaya Aura®.

Solution

1. Log in to the Avaya Aura® Device Services.
2. Go to the `/var/net-snmp` directory.
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 `service jboss restart` command to restart JBoss on System Manager.
12. Run the following command to remove the Avaya Aura® Device Services entry from System Manager:

```
sh <path_to_recoverAgent.sh> <AADS_IP_address>
```

Where, `<path_to_recoverAgent.sh>` is the full path to `recoverAgent.sh` and `<AADS_IP_address>` is the IP address of Avaya Aura® Device Services.

13. Log in to the Avaya Aura® Device Services.
14. Run the following command:

```
sudo -E $SPIRIT_HOME/scripts/utils/reinitilizeSnmpdConfiguration.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
```

15. Run the following command:

```
systemctl restart AADSSpiritAgent.service
```

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: `TLSSRV=10.103.1.39, TLSPT=1543, TLSSRVRID=0`.

Cannot upload phone firmware packages larger than 800 MB to the Utility Server after the upgrade

Condition

You increase the file size limit for phone firmware packages to 1.5 GB (1,500 MB) by using the `enableVantageFWSupport.sh` script. However, after upgrading Avaya Aura® Device Services, you cannot upload phone packages larger than 800 MB to the Utility Server.

Cause

This is the expected behavior. After upgrading, Avaya Aura® Device Services resets the file size limit for phone packages to the default value of 800 MB.

Solution

Repeat procedure [Increasing the file size limit for phone firmware packages to 1.5 GB](#) on page 252.

Synchronization with the LDAP server fails

Condition

Avaya Aura® Device Services displays the “Failed” synchronization status on the LDAP server page. The `AADS.log` and `catalina` log files contains an error indicating that LDAP synchronization failed.

Solution

1. Ensure that the LDAP server is online.
2. Ensure that the LDAP server is reachable.
3. Gather logs and contact Avaya support personnel.

Open LDAP replication fails

Condition

Open LDAP replication fails. The `/var/log/Avaya/openldap/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/openldap.log` file and ensure that it does not contain any error messages.

If the `/var/log/Avaya/openldap/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/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 232. Ensure that you select **Apply For Cluster** when importing the certificate.

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.

! Important:

You can only allocate free disk space to disk volumes if data encryption is disabled on Avaya Aura® Device Services. If data encryption is enabled, you *cannot* allocate free disk space.

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 413 and [Increasing the virtual disk size of AWS virtual machines](#) on page 415.
- 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:

```
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.

Disk and Volume Summary								
Disk					Volume			
Num	Name	Size	Free		Name	LVM Size	File System Size	Usage
1	sda	124.51	50.10	/		17.30	17.29	1.56
				/home		4.00	3.99	0.03
				/opt/Avaya		14.70	14.69	2.04
				/tmp		14.90	14.89	0.63
				/var		8.50	8.49	0.09
				/var/log		5.00	4.99	0.03
				/var/log/audit		6.00	5.99	0.03
				swap		4.00	n/a	n/a
2	sdb	70.00	0.00	/var/log/Avaya		70.00	69.98	0.11
3	sdc	40.00	0.00	/media/data		40.00	39.99	0.55
4	sdd	10.00	0.00	/media/cassandra		10.00	9.99	0.03

+ 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:

```
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:

```
sys volmgt --extend /var/log 10.5g
```

4. Run the following command to allocate all remaining disk space to a volume on the disk:

```
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:

```
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 Avaya Solutions Platform (ASP), avoid adjusting virtual hardware parameters because your adjustments could affect other applications hosted on the same ASP 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”.

Disk number	Description
Hard disk 1	Operating system and application software.
Hard disk 2	Application logs.
Hard disk 3	Application data.

 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 411.

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 deployed on AWS.

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.

Disk number	Block device	Description
Disk 1	/dev/sda1	Stores operating system and application software.
Disk 2	/dev/xvdb	Stores application logs.
Disk 3	/dev/xvdc	Stores application data.

* 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.

AWS 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:

Avaya Aura® Device Services restart is required when you change the size of disk1. If you do not modify disk1, Avaya Aura® Device Services restart is not required.

6. In the **EBS ID** field, click the ID.
AWS 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 411.

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.

Troubleshooting for OAuth2 authorization

OAuth2 authentication does not work as expected

Condition

Keycloak is not properly configured. As a result, OAuth2 authentication is not working as expected.

Solution

Verify the initial Keycloak configuration in the Avaya Aura® Device Services configuration utility and the Keycloak web administration portal. For more information about using the Keycloak web administration portal, see [Avaya Aura Device Services Single Sign-On management](#) on page 44.

Keycloak documentation is available at [Keycloak documentation](#).

Login page for the third-party identity provider is not displayed

Condition

The user cannot reach the login page for the third-party identity provider when trying to log in to Avaya Workplace Client.

Solution

- If the issue happens during the automatic configuration phase of the client, ensure that you configured DNS records on your DNS server to return an Avaya Aura® Device Services URL with the following parameter: `?preferredAuth=bearer`.
- Ensure that the machine where the client is running can connect to the address that is provided in the IDPSSODescriptor file as the SSO service URL.

An error page is displayed instead of the Login page

Condition

When the user tries to log in to Avaya Workplace Client, the user is redirected to the third-party identity provider, but an error page is displayed instead of the Login page.

Cause

The following are possible causes:

- Avaya Aura® Device Services, the third-party identity provider, and the machine where the client is running use different time synchronization services.
- The IDPSSODescriptor metadata file contains parameters that are not compatible with Avaya Aura® Device Services.
- The third-party identity provider is configured incorrectly.

Solution

- Ensure that the machine where the client is running uses the same network time synchronization service as Avaya Aura® Device Services and the third-party identity provider.
- Ensure that the IDPSSODescriptor metadata file contains only compatible parameters.
- Contact your third-party identity provider to verify configuration.

Related links

[Interoperability issues between Avaya Aura Device Services and the third-party identity provider](#) on page 421

Login credentials do not work

Condition

When the user tries to log in to Avaya Workplace Client, the user is directed to the third-party identity provider's Login page, but the user's login credentials do not work. The Login page displays information about an incorrect user name and password even though user entered the correct credentials.

Cause

Incorrect configuration of the identity provider on Keycloak.

Solution

Verify the third-party identity provider configuration on Keycloak.

Avaya Workplace Client displays an authentication error

Condition

The user can log in on the identity provider's Login page, but Avaya Workplace Client displays an authentication error.

Solution

- Verify that the mapping of the identity provider attributes are correct.
- Verify that the user record created on Keycloak contains the correct attribute values.

Related links

[Verifying the mapping of the identity provider's attributes](#) on page 420

[Verifying the attributes imported for a user](#) on page 419

Verifying the attributes imported for a user

Procedure

1. In a web browser, enter the following URL:
`https://<AADS IP or FQDN>:<AADS PORT>/auth/admin`
2. Enter the user name and the password that you created when configuring the Keycloak settings.
3. In the left area, click **Users**.
4. In the **Search** field, type the user's name and then click the magnifying glass icon.
5. Click the link in the ID column for the user to open user's properties.
6. Click the **Attributes** tab.
7. Ensure that Keycloak displays correct values for all attributes that the third-party identity provider releases.
8. If an attribute is missing or no value is set for attribute, ensure that the attribute mapping for the identity provider contains all attributes that the third-party identity provider releases.
9. Click the **Role Mappings** tab.
10. From **Client Roles**, select **aads**.
11. Ensure that the **Assigned Roles** and **Effective Roles** fields contain the correct Avaya Aura® Device Services user role for the user.
12. If the user has no user role assigned, do the following:
 - a. Ensure that the role mapping attribute in the identity provider mapping is correct.
 - b. Ensure that the identity provider's SAMLResponse contains the correct information for the role mapping attribute.

Verifying the mapping of the identity provider's attributes

Procedure

1. In a web browser, enter the following URL:
`https://<AADS IP or FQDN>:<AADS PORT>/auth/admin`
2. Enter the user name and the password that you created when configuring the Keycloak settings.
3. In the left area, click **Identity Providers**.
 Currently, the identity provider is automatically imported with the name "Shibboleth".
4. Click the **Shibboleth** link.
5. Click the **Mappers** tab.
6. Verify that the attribute mapping uses correct names for attributes that are released by the identity provider.



Tip:

You can open a decrypted SAMLResponse returned from the identity provider in a new browser window and then compare the attribute names from the SAMLResponse with attribute names that are used in the Keycloak attribute mapping.

Users cannot log in to their clients or phones using SSO

Condition

Users cannot log in to their phones or clients using SSO.

Cause

The issue might be caused by outdated public keys that Avaya Aura® Device Services uses for token validation.

Solution

1. Synchronize data with the identity provider as described in [Synchronizing data between Avaya Aura Device Services and an identity provider](#) on page 145.
2. If the problem persists, contact Avaya support.

A test user cannot log in to the identity provider

Condition

When setting up the connection between the third-party identity provider and Avaya Aura® Device Services, a test user is typically used to verify that configuration of the third-party provider and Avaya Aura® Device Services. When testing the connection, the user logs in to the identity provider, but the login fails.

Cause

The identity provider might not be correctly configured. This results in the Keycloak service storing incorrect user information. Therefore, the login fails.

Solution

Delete the user record from the Keycloak database.

1. Log in to the Keycloak web administration interface.
2. In the left area, click **Users**.
3. In the **Search** field, type the user's name and then click the magnifying glass icon.
4. In the Actions column, click **Delete** for the user to delete the user's record.

When the user log in again, Keycloak creates a new database entry with the correct user information.

Interoperability issues between Avaya Aura[®] Device Services and the third-party identity provider

Condition

Avaya Aura[®] Device Services cannot communicate with the third-party identity provider. Avaya Workplace Client cannot use SSO capabilities.

Solution

To communicate with a third-party SAML v2.0 identity provider, Avaya Aura[®] Device Services must negotiate certain SAML v2.0 parameters with the identity provider. To prevent issues, upload the identity provider's IDPSSODescriptor metadata file to Avaya Aura[®] Device Services when you enable OAuth2 authentication support on Avaya Aura[®] Device Services. The IDPSSODescriptor file automatically populates many identity provider settings on Avaya Aura[®] Device Services.

After you configure the identity provider on Keycloak, it generates the SPSSODescriptor metadata file. You can provide this file to the identity provider. You can find this file at the following location:

`https://<AADS_FQDN>/auth/realms/SolutionRealm/broker/<SAML_ALIAS>/endpoint/descriptor`. In this URL, <AADS_FQDN> is the Avaya Aura[®] Device Services front-end FQDN, and <SAML_ALIAS> is the alias of the identity provider.

You can prevent many issues by exchanging the IDPSSODescriptor and SPSSODescriptor files. However, if the metadata files contain information that is incorrect or not supported by Avaya Aura[®] Device Services, interoperability issues might still occur.

If you continue to experience problems, verify the following settings on the third-party identity provider and Avaya Aura[®] Device Services Keycloak.

- The identity provider that you use must support the Service Provider-initiated (SP-initiated) SAML v2.0 flow.
- The NameID format option must be set to emailAddress.
- The identity provider must support the HTTP POST binding.
- The identity provider and Avaya Aura[®] Device Services must use the same time synchronization service.

- Ensure that no network firewalls must block access from Avaya Aura® Device Services to the identity provider.
- The certificates specified in the identity provider's IDPSSODescription file must be valid.
- For attribute mapping, Keycloak must use the same spelling for attribute names as the identity provider. These attribute names are case-sensitive.
- The attribute names that the identity provider releases must be correctly mapped as friendly names or attribute names on Keycloak.

By default, Keycloak maps the friendly name of the attribute.

- Role information must be correctly released to Avaya Aura® Device Services, so that the correct user role can be assigned to each user.

Avaya Spaces integration

Avaya Spaces connectivity errors

The following table shows the errors that Avaya Aura® Device Services can display when it cannot connect to Avaya Spaces.

Error	Description	Solution
Avaya Spaces Host unreachable	Avaya Spaces is down.	Verify that Avaya Spaces is accessible.
	An incorrect Avaya Spaces URL is used to set up integration.	Navigate to Spaces > Configuration and ensure that Spaces URI is set to <code>accounts.avayacloud.com</code> .
Avaya Spaces configuration error, Either certificate expired OR invalid API key and secret	Avaya Spaces integration settings are incorrectly configured on Avaya Aura® Device Services.	Re-configure Avaya Spaces integration.
	An Avaya Spaces CA certificate is not valid or has expired.	Re-upload the Avaya Spaces CA certificate in the web browser you use to log in to the Avaya Aura® Device Services web administration portal.
Avaya Spaces connection failed	Network connectivity issues.	• Verify your network setup. • Gather logs and contact Avaya support personnel.

Related links

[Setting up Avaya Spaces integration](#) on page 156

Avaya Aura® Device Services does not contain the latest Avaya Spaces CA certificate

Condition

Avaya Aura® Device Services displays the OFFLINE status for Avaya Spaces on the Configuration page. The error message contains the following text:

```
Status: OFFLINE
failed on processing exception javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to
find valid certification path to requested target.
```

System Manager or other SNMP server configured in your deployment might also raise the “Raising alarm due to invalid certificates or invalid API key and secret” alarm.

Cause

Avaya Aura® Device Services does not contain the latest Avaya Spaces CA certificate in the public CA truststore.

This issue might also occur after upgrading Avaya Aura® Device Services. During the upgrade process, Avaya Aura® Device Services does not copy expired Avaya Spaces certificates into the truststore for Avaya Spaces certificates.

Solution

You must manually download the latest Avaya Spaces CA certificate and import it to the Avaya Aura® Device Services public CA truststore using the `keytool` command.

This procedure is for the Google Chrome browser. For other browsers, perform a search on documentation for exporting an SSL certificate from a website for that browser.

1. In the Google Chrome browser, navigate to <https://accounts.avayacloud.com>.
2. Press **F12** to open Developer Tools.
3. Click the **Security** tab.
4. In the Security overview section, click **View certificate**.
5. In the Certificate window, click the **Certification Path** tab.
6. Select the root CA and click **View Certificate**.
7. In the new Certificate window that is opened, click the **Details** tab.
8. Click **Copy to File**.
9. In the Certificate Export Wizard, click **Next**.
10. In the Export File Format window, select **Base-64 encoded X.509 (.CER)** and then click **Next**.
11. Select a location where you want to store the certificate and then click **Next**.
12. Click **Finish**.
13. Copy the certificate to the home directory of the administrative user on Avaya Aura® Device Services.

You can use any file transfer program, such as SFTP or SCP.

14. Log in to the Avaya Aura® Device Services CLI.

15. Run the following command:

```
sudo keytool -importcert -noprompt -alias <ALIAS_NAME> -file
<PATH_TO_CERTIFICATE> -keystore /opt/Avaya/DeviceServices/<VERSION>/CAS/<VERSION>/
cert/publicCA-ts.jks -storepass <KEYSTORE_PASSWORD>
```

In this command:

- <ALIAS> is a name of your choice that the public CA truststore will use for the Avaya Spaces CA certificate.
- <PATH_TO_CERTIFICATE> is the full path to the Avaya Spaces CA certificate.
- <KEYSTORE_PASSWORD> is the Keystore password created during Avaya Aura® Device Services deployment.

Cannot register an enterprise user on Avaya Spaces

Condition

Avaya Aura® Device Services cannot register an enterprise user on Avaya Spaces. On the Assign License page, Avaya Aura® Device Services displays the FAILED status for that user.

Cause

- Temporary connection issues between Avaya Spaces and Avaya Aura® Device Services.
- Settings configured for a user in the enterprise LDAP directory do not meet Avaya Spaces requirements.

For example, the registration process fails if the domain part of the user's email address does not match any of the domains configured for your company on Avaya Spaces.

Solution

1. Perform the registration procedure for the user again.
2. If the enterprise user is not correctly configured in your enterprise directory, do the following:
 - a. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces > Users and License > Assign License**.
 - b. Select the user and then click **Delete**.
 - c. Update settings for the user in your enterprise LDAP directory.
 - d. Re-add the user for registration.
 - e. Register the user on Avaya Spaces.

Related links

[Adding enterprise users for registration on Avaya Spaces](#) on page 165

[Registering enterprise users on Avaya Spaces](#) on page 166

[Removing an unregistered user](#) on page 167

Avaya Spaces user management operation fails

Condition

Avaya Aura® Device Services cannot:

- Update or deallocate a license for an Avaya Spaces user.
- Delete an Avaya Spaces user.

Avaya Aura® Device Services displays the FAILED status for that user in the list of Avaya Spaces users on the View and Manage page.

Solution

1. Review the error message.
2. Ensure that the connection to Avaya Spaces is up.
3. Ensure that System Manager or other SNMP server configured in your deployment does not display any Avaya Spaces-related alarms.
4. Repeat the required management operation for the user.

You must resolve any alarms related to Avaya Spaces connection before repeating the required management operation.

Related links

[Deallocating licenses](#) on page 173

[Assigning a different license to Avaya Spaces users](#) on page 174

[Removing users from your Avaya Spaces company](#) on page 175

Avaya Spaces pages blocked

Condition

Data synchronization between Avaya Aura® Device Services and Avaya Spaces is running, and all Avaya Spaces pages are blocked.

Cause

Data synchronization is stuck in the "In Progress" state.

Solution

1. On the Avaya Aura® Device Services web administration portal, navigate to **Spaces > Configuration**.
2. In the User Synchronization Update Instructions area, click **Stop**.

The synchronization status changes to "Stopped".

Stopping a running synchronization does not affect scheduled synchronization.

Logs collected using the collectlogs command are encrypted

Condition

When data encryption is enabled on Avaya Aura® Device Services, log files that you collect using the `collectlogs` command are encrypted.

Cause

The `collectlogs` command only collects Avaya Aura® Device Services logs. If logs are encrypted, this command does not provide an option to decrypt logs. To collect and encrypt decrypted logs, you must use the `collectAndDecryptLogs.sh` script.

Solution

The `collectAndDecryptLogs.sh` script allows you to collect all logs from a single node.

1. As an administrator, log in to the CLI of the Avaya Aura® Device Services node from which you want to collect logs.
2. Run the following commands:

```
cdto misc
sudo ./collectAndDecryptLogs.sh
```

Avaya Aura® Device Services collects all logs from the node, decrypts them, and stores the decrypted logs in a TAR archive in the following directory:

```
/opt/Avaya/DeviceServices/<AADS VERSION>/CAS/<AADS VERSION>/log-  
collection/collected-logs/
```

3. **(Optional)** Download the archive with log files to your machine using a file transfer program, such as SFTP or SCP.
4. If you need to collect logs from other nodes, repeat the steps above for the required nodes in the cluster.

Related links

[collectlogs](#) on page 445

Avaya Workplace Client cannot connect to Avaya Aura® Device Services

Condition

Avaya Workplace Client is unable to connect to Avaya Aura® Device Services to complete the mutual authentication for client identity certificates.

Cause

On Avaya Aura® Device Services, on the HTTPS Clients screen, the administrator has set the Client-Device Certificate Policy as Required.

Solution

On the HTTP Clients screen, the administrator must set the Client-Device Certificate Policy as None.

Avaya Workplace Client cannot connect to Avaya Aura® Device Services when the secure connection is enabled

Condition

Avaya Workplace Client cannot connect to Avaya Aura® Device Services when the secure client connection is enabled on Avaya Aura® Device Services. Avaya Workplace Client displays a 400 Bad Request error. For example:

HTTP Status 400 - Bad Request

Type: Status report

Message: client has unsupported browser extension

Description: The server cannot or will not process the request due to something that is perceived to be a client error.

Cause

When the secure client connection is enabled, Avaya Aura® Device Services rejects a connection if a client provides an invalid certificate. Avaya Aura® Device Services also rejects a connection if a client certificate contains unsupported critical extensions, is expired, or if the start date of the certificate is in the future.

Solution

Ensure that the client uses a valid certificate that does not contain unsupported critical extensions to connect to Avaya Aura® Device Services.

Cannot access Avaya Aura® Device Services resources over port 443

Condition

You cannot access Avaya Aura® Device Services resources located at the following URLs:

- `https://<AADS_NODE_IP>:443/acs/resources/<RESOURCE_NAME>`
- `https://<AADS_NODE_IP>/acs/resources/<RESOURCE_NAME>`

when accessing them using the node IP address and default front-end port 443. The virtual IP address is configured on Avaya Aura® Device Services.

Cause

This is the expected behavior. If the virtual IP address is enabled, Avaya Aura® Device Services blocks access to the resources over port 443 for node IP addresses. This restriction applies to standalone and cluster deployments.

Solution

- Use either the virtual IP address or the front-end FQDN to access the resources over port 443.
- **(Optional)** In a standalone deployment, you can disable the virtual IP address.

The location of automatic backups has changed after the upgrade

Condition

After the upgrade, Avaya Aura® Device Services uses the default location for automatic backup files instead of the location that you defined.

Cause

This is the expected behavior.

Solution

Configure the required location for automatic backups as described in [Changing the location of automatic backups](#) on page 354.

Disk space full on one node disables the service on all nodes

Condition

When the disk space is full on one node, all the cluster nodes go down and an alarm is triggered.

Solution

When the disk space alarm is triggered on the Avaya Aura® Device Services server, check which disk on the node is full and manually clear the unnecessary files.

Running the Cassandra repair manually

About this task

If a Cassandra node contains inaccurate information, Avaya Aura® Device Services fixes this issue during the next automatic database repair operation. Avaya Aura® Device Services performs automatic repairs on a weekly basis. If you do not want to wait until the next automatic repair, you can run the Cassandra repair process manually.

! Important:

- Avaya recommends that you use the automatic repair functionality to fix database issues whenever possible.
- The repair process might impact the Avaya Aura® Device Services performance. Therefore, ensure to run the repair outside of business hours in your enterprise.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator.
2. Run the following command:

```
nodetool repair -full
```

The repair process might take some time to complete.

Related links

[Auto Configuration Failure: 500 Internal Server Error](#) on page 429

Auto Configuration Failure: 500 Internal Server Error

About this task

In LDAP attribute mapping, **SMGRLoginName** is by default mapped to the **userprincipalName**. If the **SMGRLoginName** mapped attribute is null for a given user in the LDAP and the auto configuration api is hit to fetch the user configuration, it results in failure.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Server Connections > LDAP Configuration > Enterprise LDAP Server Configuration > Modify Attribute Mappings**.
2. For the **SMGRLoginName** field under **Enterprise Directory Mappings > Modify LDAP Attribute Mappings** if the default value under the **Custom Field Name** column is **userprincipalName**:
 - a. Go to **LDAP** server and check the user configuration and the mapped attribute under **userprincipalName**.
 - b. If the attribute is blank, modify the mapping in the Avaya Aura® Device Services web administration portal.

Related links

[Running the Cassandra repair manually](#) on page 429

RHEL single-user mode

Single-user mode is a maintenance mode available on Linux-based operating systems. In single-user mode, the operating system only starts certain services for troubleshooting and maintenance operations. In the single-user mode, you can perform operating system-level troubleshooting operations, such as repairing the file system or starting or stopping services. For more information about the use of the single-user mode, refer to the official RHEL documentation.

In single-user mode, network services are not available. Therefore, you cannot use Avaya Aura® Device Services functionality on a node that operates in single-user mode.

Avaya Aura® Device Services supports single-user mode only in a VMware-based environment for both OVA-based and software-only deployment types. You cannot enable single-user mode on Amazon Web Services because you cannot change the boot sequence of the operating system in Cloud environments.

Booting the RHEL into single-user mode

About this task

You can use single-user mode of the RHEL operating system to perform operating system-level troubleshooting and maintenance tasks. The Avaya Aura® Device Services functionality is unavailable in single-user mode.

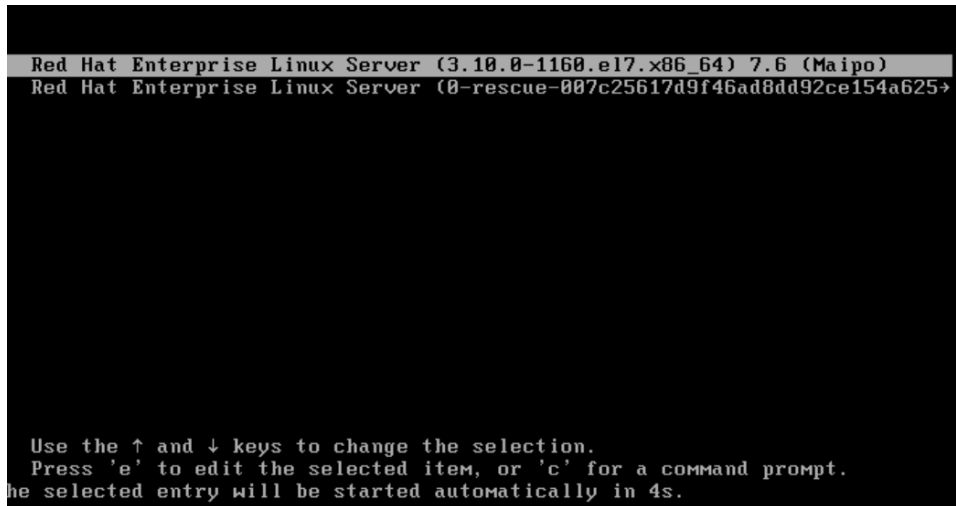
You can only enable single-user mode in VMware-based environments.

In VMware OVA-based deployments, single-user mode is password-protected. The default password is the administrator password that you configure when installing Avaya Aura® Device Services. When you enable single-user mode for the first time, you must change the default password.

Procedure

1. From vCenter, select your Avaya Aura® Device Services virtual machine.
2. On the Summary tab, click **Launch Web Console**.
3. Reboot your virtual machine.

4. When vCenter displays the GRUB boot menu, select the appropriate kernel version and then press `e`.



5. When prompted to enter the user name, enter `root`.
6. When prompted to enter the password, do one of the following:
 - If you boot into single-user mode for the first time, type the administration password that you configured when installing Avaya Aura® Device Services, and then configure a password for single-user mode.
Avaya Aura® Device Services does not enforce complexity rules for single-user mode passwords.
 - If you have already used single-user mode, type the password that you configured for single-user mode.
7. When Avaya Aura® Device Services displays the Setparams window, navigate to the line that starts with `linux16` using the navigational keys.
8. At the end of the line, type the Space character (" ") and then type the following entry:
`rd.break console=tty1`
9. Press `Ctrl+X`.

After the reboot, RHEL boots into the single-user mode.

Changing the password for single-user mode

About this task

You can change the password for single-user mode from the Avaya Aura® Device Services CLI. You do not need to log in to single-user mode to change the single-user mode password.

Avaya Aura® Device Services does not enforce any complexity rules for single-user mode passwords, therefore you can use any password that you want.

Procedure

1. Log in to the Avaya Aura® Device Services CLI as an administrator using an SSH connection.
2. Run the following command:

```
sudo /opt/Avaya/bin/manageOSPassword.sh -p
```
3. Follow the system prompts to change the single-user mode password.

Exiting the single-user mode

About this task

After performing maintenance tasks in single-user mode, switch back to normal Avaya Aura® Device Services operational mode.

Procedure

When in the single-user mode, run the following command:

```
reboot -f
```

After the reboot, Avaya Aura® Device Services starts in normal mode.

Client login failure when Identity provider link already exists in Keycloak

Condition

Users cannot log in to client.

Cause

The Identity Provider (IdP) link in Keycloak account already exists.

Solution

1. To **Create a New Flow**, do the following:
 - a. Navigate to **Authentication > Flows**.
 - b. Click **Create** and give the name for the flow as `Auto Link Identity Provider Flow`.
 - c. For **Flow type**, select **Basic Flow**.
 - d. Click **Add execution > Automatically set existing user > Add**.
2. To **Configure Authenticators**, do the following:
 - a. For **Automatically set existing user**, select **Alternative**.
 - b. For **Create User if Unique**, select **Alternative**.

*** Note:**

Do not add any authenticators or subflows to this configuration.

3. To **Update the Identity Provider**, do the following:
 - a. Navigate to **Identity Providers** and select the required provider.
 - b. Enable **Trust Email**.
 - c. For **First login flow**, change to **Auto Link Identity Provider Flow** as given in [1.b](#) on page 432.
 - d. For **Sync Mode**, select **Force**.
4. Click **Save**.

Secured LDAP user federation with keycloak error occurs during configuration settings

Cause

The keycloak uses the default Java 1.8 as truststore instead of the Java 17 truststore.

Solution

1. To obtain LDAP server certificate, do the following:
 - a. Export the LDAP server certificate:


```
openssl
```
 - b. View the LDAP server certificate:


```
echo | openssl s_client -connect ldap.example.com:636 -showcerts
```
 - c. Copy the certificate to a file. For example: `ldap-server.crt`
2. Import the LDAP certificate into keycloak truststore:


```
keytool -importcert -file ldap-server.crt -alias ldap-server -keystore /path/to/keycloak/conf/cacerts -storepass changeit
```
3. To configure LDAP in keycloak, do the following:
 - a. Log into keycloak admin console.
 - b. Navigate to the required realm.
 - c. Click **User Federation > Add LDAP provider**.
 - d. In the **Connection URL** field, enter one of the following:
 - For IP address, enter `ldaps://10.133.98.168:636`
 - For FQDN, enter `ldaps://aadsldap.gsc.com:636`
 - e. Click **Test Connection**

- f. Enter **Bind DN** and **Bind credentials**.
- g. Click **Test authentication**.
Successfully connected to LDAP is displayed.
- h. Under **LDAP searching and updating** section, do the following:
 - Enter **User DN**. For example: OU=uc7_smg,DC=gsc,DC=com.
 - For **Username LDAP attribute**, enter one of the following:
 - sAMA account name
 - User principal name
 - Email address.
- * **Note:**
 Name of the LDAP attribute, which is mapped as Keycloak username. For many LDAP server vendors it can be 'uid'. For Active directory it can be 'sAMAccountName' or 'cn'. The attribute should be filled for all LDAP user records you want to import from LDAP to Keycloak.
- i. Enable **Periodic full sync**.
4. Click **Save**.

Users cannot log in to the client due to expiry of third-party Identity provider certificate

Condition

The **Validate Signature** is enabled in the keycloak SAML settings. Users cannot log in to the client when authenticating through an expired third-party Identity Provider certificate.

Cause

The third-party Identity provider certificate is expired.

Solution

1. Log in to the Keycloak Admin console.
2. Click **SolutionRealm > Identity Provider**.
3. In **Identity Providers**, select the required provider.
4. Enable **Validate Signature**.
5. Under **SAML Settings**, in **Validating X509 Certificates**, delete the expired certificate and copy and paste the new certificate.
6. Click **Save**.

Chapter 21: Migrating Avaya Aura® Device Services from VMware to ASP R6.0.x (KVM on RHEL 8.10)

Migrating Avaya Aura® Device Services from VMware to ASP R6.0.x (KVM on RHEL 8.10)

About this task

Use this procedure to migrate Avaya Aura® Device Services R10.2.x ASP R5.x (VMware) to Avaya Aura® Device Services R10.2.x ASP R6.0 (KVM on RHEL).

When migrating, ensure to match the Avaya Aura® Device Services version from backup to restore. Perform the backup and restore on the same Avaya Aura® Device Services version.

Procedure

1. Note-down the existing VMware details.
For more information, see [Obtaining existing VMware details](#) on page 436.
2. Perform prerequisite tasks to migrate Avaya Aura® Device Services from VMware to KVM.
For more information, see [Checklist of prerequisite tasks to migrate Avaya Aura Device Services from VMware to ASP R6.0.x \(KVM on RHEL 8.10\)](#) on page 436.
3. Install ASP R6.0.x (KVM on RHEL 8.10).
For more information, see *Installing the Avaya Solutions Platform 130 Series* at <https://support.avaya.com/css/public/documents/101091802>.
4. Deploy Avaya Aura® Device Services on KVM host.
For more information, see *Deploying Avaya Aura® Device Services*.
5. Restore Avaya Aura® Device Services Backup.
For more information, see [Restoring Avaya Aura Device Services in a standalone environment](#) on page 358 and [Restoring an Avaya Aura Device Services cluster](#) on page 360.
6. Run the command "`svc aads status`" to verify the restored data.

Obtaining existing VMware details

About this task

Obtain the configuration details of VMware and use them for ASP R6.0.x (KVM on RHEL 8.10).

For module-specific details, see [Obtaining Avaya Aura Device Services network configuration details](#) on page 437

Use this procedure to obtain the network IP interface details.

Procedure

1. Log in to ESXi CLI, run the following commands:

- # esxcli network ip interface ipv4 get: note down IPv4 network IP interface details.
- # esxcli network ip interface ipv6 get: note down IPv6 network IP interface details.

```
[root@localhost:~]
[root@localhost:~] esxcli network ip interface ipv4 get
Name IPv4 Address IPv4 Netmask IPv4 Broadcast Address Type Gateway DHCP DNS
-----
vmk0 10.10.10.10 255.255.255.0 10.10.10.255 STATIC 10.10.10.1 false
[root@localhost:~]
[root@localhost:~]
[root@localhost:~]
[root@localhost:~] esxcli network ip interface ipv6 get
Name IPv6 Enabled DHCPv6 Enabled Router Adv Enabled DHCP DNS Gateway
-----
vmk0 true false true false ::
```

2. Login to ESXi vSphere or vCenter and note down the VMware License serial number.

Checklist of prerequisite tasks to migrate Avaya Aura® Device Services from VMware to ASP R6.0.x (KVM on RHEL 8.10)

Perform the tasks in this checklist to migrate Avaya Aura® Device Services R10.2.x ASP R5.x (VMware) to ASP R6.0 (KVM).

No.	Task	Description	✓
1	Check the disk encryption status	See Viewing data encryption status on page 310.	
2	Record the network configuration details	See Obtaining Avaya Aura Device Services network configuration details on page 437.	

No.	Task	Description	✓
3	Check the FIPS status	Run the command <code>sys secconfig --fips --query</code> in Avaya Aura® Device Services CLI.	
4	Check the system layer version	See sys versions command on page 450.	
5	Check the application layer version	Log in to the virtual machine using the administrative user ID and run the command <code>svc aads swversion</code> to check the application layer version.	
6	Back up Avaya Aura® Device Services	See Backing up Avaya Aura Device Services on page 351.	

Obtaining Avaya Aura® Device Services network configuration details

Before you begin

Determine the keystore password you want to use when installing Avaya Aura® Device Services Release 10.2.x.

Procedure

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 -nr | 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.

Chapter 22: Resources

Documentation

The following table lists related documentation. All Avaya documentation is available at <https://support.avaya.com>. Many documents are also available at <https://documentation.avaya.com/>.

Title	Use this document to:	Audience
Implementing		
<i>Deploying Avaya Aura® Device Services</i>	Deploy Avaya Aura® Device Services.	Sales engineers, solution architects, implementation engineers, support personnel
<i>Deploying Avaya Aura® Session Manager</i>	Deploy the Session Manager OVA.	Sales engineers, solution architects, implementation engineers, support personnel
Administering		
<i>Administering Avaya Aura® Device Services</i>	Administer Avaya Aura® Device Services.	System administrators, support personnel
<i>Administering Avaya Aura® Session Manager</i>	Administer the Session Manager interface.	System administrators, support personnel
<i>Planning for and Administering Avaya Workplace Client for Android, iOS, Mac, and Windows</i>	Perform system planning and configuration for: • Avaya Workplace Client for Android • Avaya Workplace Client for iOS • Avaya Workplace Client for Mac • Avaya Workplace Client for Windows	System administrators, support personnel
<i>Using Avaya Spaces</i>	Administer Avaya Spaces.	System administrators, support personnel
Using		

Title	Use this document to:	Audience
<i>Using Avaya Device Enrollment Services to Manage Endpoints</i>	Use Device Enrollment Services to manage endpoints or devices.	Non-Avaya users, such as service providers and resellers
Other		
<i>Avaya Aura® Device Services Data Privacy Controls Addendum</i>	Understand how Avaya Aura® Device Services processes user's personal data.	Customers, service providers, system administrators, support personnel
<i>Port Matrix for Avaya Aura® Device Services</i>	Understand ports for Avaya Aura® Device Services.	Solution architects, implementation engineers, system administrators, support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.
This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.
For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click  to display the search results.

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at <https://documentation.avaya.com>. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the [Avaya Support website](#).

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** () in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.
You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click < or > next to the document title to navigate to the previous topic or the next topic.
- Click **Share** () to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** (). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

You can do the following:

- Create, rename, and delete a collection.
- Set a collection as the default or favorite collection.
- Save a PDF of the selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collections that others have shared with you.
- Click **Watch** () to add a topic to your watchlist so you are notified when the content is updated or removed.

- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

You can do the following:

- Enable **Email notifications** to receive email alerts.
 - Unwatch the selected content or all topics.
- Send feedback for a topic.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to <https://support.avaya.com/> and do one of the following:
 - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
 - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
 - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
 - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at <https://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service

request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.
- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

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.

collectlogs

The **app collectlogs** command enables you to collect and download the logs from an Avaya Aura® Device Services node. For example, if you run the following command, two logs will be downloaded from the 10.10.10.1 node:

```
$ app collectlogs collect -n 2 -ip 10.10.10.1
```

By default, if details are not specified, the system will download all 20 logs from the local node.

For more information about the available options, run the following command:

```
$ app collectlogs h
```

Note:

Avaya recommends that you collect and download logs using the web administration portal. For more information, see [Changing a logging level](#) on page 334 and [Downloading logs](#) on page 336.

Related links

[Logs collected using the collectlogs command are encrypted](#) on page 426

clitool-accs

The `clitool-accs` utility provides multiple usage possibilities, depending on which parameters the utility receives in the command line.

The utility is located in the `/opt/Avaya/DeviceServices/<version>/CAS/<version>/misc` directory.

Usage example

Run the `clitool-accs.sh` utility with the appropriate parameters. To view the command options, run the `clitool-accs.sh` utility without any parameters. You must run this utility with the `sudo` privileges.

* Note:

The `clitool-accs` utility does not create report directories automatically. Before running the utility, you must run the following commands to create a report directory and set the read, write, and execute permissions to this directory:

```
mkdir <report_directory>
chmod 777 <report_directory>
```

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 the `/opt/Avaya/DeviceServices/<version>/CAS/<version>/bin` directory.

* Note:

You can also run the `app status` command.

```
[avaya@AWSDev-14 /]$ sudo /opt/Avaya/DeviceServices/8.0.1.0.243/CAS/8.0.1.0.243/bin/statusAADS.sh
[sudo] password for avaya:
2020-01-09_11:00:04 Displaying status for Avaya Aura Device Services Application
2020-01-09_11:00:04 ulimit file count ..... [ OK ]
2020-01-09_11:00:04 ulimit process count ..... [ OK ]
2020-01-09_11:00:04 iptables status ..... [ OK ]
2020-01-09_11:00:04 RecoveryManager Watchdog status ..... [ OK ]
2020-01-09_11:00:04 RecoveryManager Service status ..... [ OK ]
2020-01-09_11:00:05 net-SNMP status ..... [ OK ]
2020-01-09_11:00:05 RecoveryManager status ..... [ OK ]
2020-01-09_11:00:05 AADSKeepalived status ..... [ INACTIVE ]
2020-01-09_11:00:05 AADSTomcat status ..... [ OK ]
2020-01-09_11:00:05 AADSNginx status ..... [ OK ]
```

Checking the Avaya Aura® Device Services status from the CLI

About this task

You can check whether the services of a local Avaya Aura® Device Services node are active using the command line interface. If Avaya Aura® Device Services indicates that any service is inactive, then the node is not working as expected.

Procedure

1. Log in to the Avaya Aura® Device Services CLI using an SSH connection.
2. Type `svc aads status`.

Result

The system displays the current status of services of the Avaya Aura® Device Services node.

- If a service is active, its status is “Running”.
- If a service is currently inactive, its status is “Not running”. In this case, Avaya Aura® Device Services also displays additional status information:
 - “Inactive”: The service is turned off.
 - “Activating”: The service is starting or restarting.

The following is an example of the command output where all services are active:

```
[admin@aads ~]$ svc aads status
```

Status of Avaya Aura Device Services Application

AADSTomcat	Running	n/a	11818
AADSNginx	Running	n/a	10246
AADSCassandra	Running	n/a	8121
AADSPostgres	Running	n/a	8767
AADSKeepalived	Running	n/a	10322
httpd	Running	n/a	9750
slapd	Running	n/a	13376
keycloak	Running	n/a	23857

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
        Command syntax (this help)

    -hh, --hhhelp
        Verbose help

Available commands:

    secconfig      [Manage security settings]
    versions      [Query version information]
    smcvemgt       [Manage Spectre/Meltdown patches]
    ipv6config     [Manage server IPv6 configuration]
    extension      [Manage system layer extensions]
    passwdrules    [Manage password rules]
    encryptionStatus [Show disk encryption status]
    encryptionPassphrase [Manage disk encryption passphrases]
    encryptionLocalKey [Manage disk encryption local key]
    encryptionRemoteKey [Manage disk encryption remote keys]

Command invocation syntax:
    sys <command> <arguments>

Command syntax:
    sys <command> -h

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

! Important:

For software-deployments, only the following system layer commands are available:

- **sys versions**
- **sys passwdrules**

Other system layer commands are unavailable.

Verbose help information

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

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

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

secconfig
    Manages security-related settings.

versions
```

```

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

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

ipv6config
    Manages configuration of server-level IPv6.

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

passwdrules
    Manages the configuration of password rules.

encryptionStatus
    Show the status of disk encryption.

encryptionPassphrase
    Adds, changes, and removes disk encryption passphrases, and
    lists the configuration of disk encryption keys.

encryptionLocalKey
    Enables and disables disk encryption local key.

encryptionRemoteKey
    Adds and removes remote key servers (tang servers), and
    list the configuration of disk encryption keys.

[admin@server-dev ~]$

```

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

sys secconfig command

sys secconfig provides access to the **secconfig** command, which existed in previous releases.

This command is only available for OVA-based deployments.

The following is an example of this command:

```

[admin@server4950aads ~]$ sys secconfig --hhelp

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

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

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

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

--fips < --enable | --disable | --query >

```

```
Enables, disables, and queries the current state of FIPS on the system.

[admin@server4950aads ~]$
```

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

[admin@server4889aads ~]$
```

sys volmgt command

Syntax help: sys volmgt --help

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

! Important:

- The **sys volmgt** command is only available if data encryption is *disabled* on Avaya Aura® Device Services. If data encryption is enabled, this command is unavailable and you cannot allocate free disk space to disk volumes.
- This command is only available for OVA-based deployments.

The following provides the command line syntax for this command:

```
[admin@server4889aads ~]$ sys volmgt --help

Syntax:
  --help,                -h
  --hhhelp,              -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 --hhhelp

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

```
[admin@server4889aads ~]$ sys volmgt --hhhelp

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.

--hhhelp, -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 or 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 mebibytes, "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 ~]$
```

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							
Disk				Volume			
Num	Name	Size	Free	Name	LVM Size	File System Size	Usage
2	sdb	25.00	0.00	/home	4.00	3.94	1.49
				/opt/Avaya	21.00	20.67	1.27
3	sdc	10.00	0.00	/media/data	10.00	9.84	0.15

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								
Disk				Volume				
Num	Name	Size	Free	Name	LVM Size	File System Size	System Usage	
1	sda	124.51	50.10	/	17.30	17.29	1.56	
				/home	4.00	3.99	0.03	
				/opt/Avaya	14.70	14.69	2.04	
				/tmp	14.90	14.89	0.63	
				/var	8.50	8.49	0.09	
				/var/log	5.00	4.99	0.03	
				/var/log/audit	6.00	5.99	0.03	
				swap	4.00	n/a	n/a	
2	sdb	70.00	0.00	/var/log/Avaya	70.00	69.98	0.11	
3	sdc	40.00	0.00	/media/data	40.00	39.99	0.55	
4	sdd	10.00	0.00	/media/cassandra	10.00	9.99	0.03	

sys smcvemgt command

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

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

* Note:

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

This command is only available for OVA-based deployments.

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 **smcvmgt** command, see <https://access.redhat.com/articles/3311301>. For more information about the Spectre and Meltdown vulnerabilities, see <https://access.redhat.com/security/vulnerabilities/speculativeexecution>.

Syntax help: sys smcvmgt --help

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

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

Version 1.2

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

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

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

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

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

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

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

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

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

Syntax:
  --help,      -h
                  Provide terse help.

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

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

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

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

If "enabled" is specified, then both v2 and v3 are enabled, with v2 set to kernel default behavior. If "disabled" is specified, then both v2 and v3 are disabled. Otherwise, kernel patches are enabled or 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 smcvemgt enabled
sys smcvemgt v2=default v3=enabled
```

The following two commands are equivalent:

```
sys smcvemgt disabled
sys smcvemgt v2=disabled v3=disabled
```

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

sys smcvemgt usage examples

Command for querying current tunable settings

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

```
sys smcvemgt --query
```

Command for enabling patches with default settings

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

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

Commands for enabling patches with specific settings

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

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

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

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

Command for disabling patches

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

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

Command for disabling patches for a specific vulnerability

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

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

sys ipv6config command

The **sys ipv6config** command is used to configure IPv6 at the system level. You can do the following:

- Configure IPv6 interactively or non-interactively. When you configure IPv6 interactively, Avaya Aura® Device Services prompts you to enter the IPv6 address, network prefix, and default gateway. When you configure IPv6 non-interactively, you must provide these settings as command options.
- Review the IPv6 configuration.
- Delete the IPv6 networking configuration.

For more information about the supported options, run this command with the **-h** argument. The following is an example:

```
[admin@aaads ~]$ sys ipv6config -h
Usage:
  ipv6config show
    Shows the server's IPv6 networking configuration.
```

```

    ipv6config set [options]
        Sets, or updates, the server's IPv6 networking configuration. If no
        options are specified, then data is collected interactively. Existing
        configuration is used for any non-specified IPv6 configuration items.
        A default network prefix of 64 is used if a prefix cannot be resolved.
        Specify "-h" for a list of available options.

    ipv6config delete
        Deletes the server's IPV6 networking.

Options:
    -h, --help                show this help message and exit
    --ip=ADDRESS[/PREFIX]     IPv6 interface address.
    --prefix=PREFIX           IPv6 prefix. If a prefix is also specified in the --ip
                             option, then this option takes precedence.
    --gw=GATEWAY_ADDRESS     IPv6 default gateway address.

```

This command is only available for OVA-based deployments.

Example: interactive configuration

The following example shows IPv6 configuration in interactive mode:

```

[admin@aaads bin]$ sys ipv6config set

Interface IPv6 address ('q' to quit) [] => 2a07:2a42:adc0:112::fa
IPv6 network prefix ('q' to quit) [64] =>
Interface IPv6 default gateway ('q' to quit) [] => 2a07:2a42:adc0:112::1/64

The server IPv6 configuration will be updated to the following and networking
will be restarted:

    Interface address : 2a07:2a42:adc0:112::fa
    Prefix             : 64
    Default gateway    : 2a07:2a42:adc0:112::1
    Network            : 2a07:2a42:adc0:112::/64

Confirm (y/n) => y

Applying configuration:

    Interface address : 2a07:2a42:adc0:112::fa
    Prefix             : 64
    Default gateway    : 2a07:2a42:adc0:112::1
    Network            : 2a07:2a42:adc0:112::/64

Restarting networking.
Done

```

passwdrules command

Description

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

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

Syntax

```

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

```

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

Syntax help

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

Options

Option	Description
<code>--diff=INTEGER</code>	Number of characters in the new password that must not be present in the old password.
<code>--min-len=INTEGER</code>	Minimum length of the password. The default minimum length is 15 characters.
<code>--min-digs=INTEGER</code>	Minimum number of digits in the password.
<code>-min-upper=INTEGER</code>	Minimum number of uppercase characters in the password.
<code>--min-lower=INTEGER</code>	Minimum number of lowercase characters in the password.
<code>--min-other=INTEGER</code>	Minimum number of special characters in the password.  Important: Avaya Aura® Device Services supports the following special characters: !, @, #, %, \$, ^, *, ?, and _.
<code>--min-class=INTEGER</code>	Minimum number of character classes that must be present in the password. The character classes are: • Digits • Uppercase characters • Lowercase characters • Special characters
<code>--max-repeat=INTEGER</code>	Maximum allowed number of consecutively repeated characters. For example, if you set this parameter to 3, then the following password is invalid: paaassword, because a is repeated three times.
<code>--max-class-repeat=INTEGER</code>	Maximum allowed number of consecutively repeated characters of the same class. For example, if you set this parameter to 3, then the pas1sw2or3d password is invalid, because the first three characters, which are p, a, and s, belong to the same character class.

Option	Description
<code>--history=INTEGER</code>	Number of previous passwords that must not match the new password.

Example

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

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

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

Data encryption commands

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

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

! Important:

- In AWS deployments, you enable data encryption on AWS itself. Therefore, you cannot use the system layer commands for disk encryption management in AWS deployments.
- These commands are only available for OVA-based deployments.

encryptionPassphrase command

Description

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

Syntax

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

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

encryptionStatus command

Description

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

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

Syntax

```
sys encryptionStatus
```

encryptionRemoteKey command

Description

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

Syntax

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

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

encryptionLocalKey command

Description

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

Syntax

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

enable	Enables the local key store.
disable	Disables the local key store.

runUserDiagnostics tool

The **runUserDiagnostics** tool is used with the **clitool-acs.sh** tool for collecting and dumping user and contact-related information.

You can run the command for a user by:

- specifying the user's email ID
- specifying a filename that contains comma separated email IDs of more than one user

The tool generates an excel file for each user. The file name contains the email address of the user to distinguish the file name for each user.

Syntax

```
sudo ./clitool-acs.sh runUserDiagnostics [-e email_address] [-f
<absolute_filepath><filename>] [-d <email_address>] [-a]
```

e	Creates an excel file in <code>/opt/Avaya/</code> directory that contains contact-related information for the email ID specified
f	Creates excel files in <code>/opt/Avaya/</code> directory that contains contact-related information for each email ID specified in the text file
d	Deregisters a registered user and removes all user related data from Avaya Aura® Device Services
a	Creates an excel file in <code>/opt/Avaya/</code> directory that contains the number of contacts in Session Manager and Avaya Aura® Device Services for all registered Avaya Aura® Device Services users
email_address	Email address of a user
filename	Filename containing comma separated email IDs. The file must be accessible from the <code>misc</code> directory for <code>clitool</code> and stored under <code>opt/Avaya</code> or a sub-directory.
absolute_filepath	Absolute filepath of the directory where the filename containing comma separated email IDs is stored.

Example

The following examples show how the **runUserDiagnostics** tool can be used with the available features.

```
sudo ./clitool-acs.sh runUserDiagnostics -e email1@domain.com
```

Creates an output file for containing contact related information for email1@domain.com.

```
sudo ./clitool-acs.sh runUserDiagnostics -f /opt/Avaya/filelist.txt
```

Creates output files containing contact related information for every email specified in `/opt/Avaya/filelist.txt`.

```
sudo ./clitool-acs.sh runUserDiagnostics -d email1@domain.com
```

Deregisters email1@domain.com and removes all data related to this user from Avaya Aura® Device Services.

```
sudo ./clitool-acs.sh runUserDiagnostics -a
```

Checks the number of contacts in Session Manager and Avaya Aura® Device Services for all registered Avaya Aura® Device Services users and creates a file `opt/Avaya/Contacts.xls`.

Files

The following files are associated with the `runUserDiagnostics` tool:

- `opt/Avaya/DeviceServices/version/CAS/version/misc/clitool-acs.sh`
- `/opt/Avaya/Contact.xls`

enableVantageFWSupport.sh command

Description

The `enableVantageFWSupport.sh` command is used to configure the file size limit for phone firmware packages you can upload to the Utility Server. By default, the file size limit is 800 MB. You can increase it to 1,500 MB (1.5 GB).

Although the script name references Avaya Vantage™, the script increases the firmware package size limit for *all* phone models that the Utility Server supports.

Run the `enableVantageFWSupport.sh` script from the `/opt/Avaya/DeviceServices/<version>/CAS/<version>/misc` directory. You can navigate to this directory by using the `cdto misc` command.

Syntax

```
sudo ./enableVantageFWSupport.sh [--install | --status | --rollback]
```

- install** Increases the file size limit for phone firmware packages to 1.5 GB.
- status** Displays the file size limit currently configured on Avaya Aura® Device Services.
- rollback** Sets the file size limit for phone firmware packages to its default value of 800 MB.

https_healthCheck.sh command

Description

The `https_healthCheck.sh` command is used to enable or disable HTTPS support for health checks for remote nodes. By default, Avaya Aura® Device Services does not support HTTPS for health checks.

Run the **https_healthCheck.sh** script from the `/opt/Avaya/DeviceServices/<version>/CAS/<version>/misc` directory. You can navigate to this directory by using the **cdto misc** command.

Syntax

```
sudo ./https_healthCheck.sh [--enable | --disable | -h]
```

- enable** Enables HTTPS support for health checks.
- disable** Disables HTTPS support for health checks.
- h** Displays information about command usage.

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.

Alias	Description
app	Provides commands for application-specific tasks such as backup, restore, and view status. If you type app without arguments, Avaya Aura® Device Services displays the available subcommands. For example, to create a backup, run the app backup command.
svc	Provides commands for managing services, such as starting, stopping, and viewing status. If you type svc without arguments, Avaya Aura® Device Services displays the available subcommands. For example, to start the services of Avaya Aura® Device 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, Avaya Aura® Device Services displays the available subcommands. For example, the following commands give the same results: <code>cd /opt/Avaya/DeviceServices/<version>/CAS/<version></code> <code>cdto cas</code>

app commands

The following table displays the available **app** commands.

Command	Description
app install	Runs the staged application installer.

Command	Description
<code>app status</code>	Displays Avaya Aura® Device Services status information.
<code>app configure</code>	Runs the configuration utility.
<code>app listnodes</code>	Displays information about the server nodes.
<code>app collectlogs</code>	Collects logs from an Avaya Aura® Device Services node.
<code>app backup</code>	Creates backup files on all Avaya Aura® Device Services nodes.
<code>app restore</code>	Restores Avaya Aura® Device Services data from a backup file on the current node.
<code>app upgrade</code>	Upgrades Avaya Aura® Device Services on the current node.
<code>app rollback</code>	Aborts the upgrade procedure and rolls back to the previously installed Avaya Aura® Device Services release.
<code>app removeinactive</code>	Removes the inactive Avaya Aura® Device Services version.
<code>app uninstall</code>	Uninstalls Avaya Aura® Device Services.

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.

Command	Navigation target
<code>cdto base</code>	<code>/opt/Avaya</code>
<code>cdto root</code>	<code>/opt/Avaya/DeviceServices</code>
<code>cdto active</code>	<code>/opt/Avaya/DeviceServices/<version></code>
<code>cdto cas</code>	<code>/opt/Avaya/DeviceServices/<version>/CAS/<version></code>
<code>cdto misc</code>	<code>/opt/Avaya/DeviceServices/<version>/CAS/<version>/misc</code>
<code>cdto bin</code>	<code>/opt/Avaya/DeviceServices/<version>/CAS/<version>/bin</code>
<code>cdto config</code>	<code>/opt/Avaya/DeviceServices/<version>/CAS/<version>/config</code>
<code>cdto logs</code>	<code>/opt/Avaya/DeviceServices/<version>/logs</code>
<code>cdto ilogs</code>	<code>/opt/Avaya/DeviceServices/.AADSInstallLogs</code>
<code>cdto tlogs</code>	<code>/opt/Avaya/DeviceServices/<version>/tomcat/<Tomcat version>/logs</code>
<code>cdto cassandra</code>	<code>/opt/Avaya/DeviceServices/<version>/cassandra/<Cassandra version></code>

Command	Navigation target
<code>cdto openldap</code>	<code>/opt/Avaya/DeviceServices/<version>/CAS/<version>/openldap</code>

Using the Tmux utility

About this task

Avaya Aura® Device Services resets idle SSH sessions after a certain period of time. This might affect lengthy CLI operations, such as Avaya Aura® Device Services installation or backup. If the connection with the SSH terminal is reset while installation or backup operations are in progress, you must restart these operations. To prevent this issue, you can start a Tmux session before performing a lengthy operation. Commands and processes that you run from a Tmux session continue to run even if the connection with the SSH terminal is reset. Therefore, you can re-connect to the Tmux session and complete the operation.

Procedure

1. To start a Tmux session, run the following command from the Avaya Aura® Device Services CLI:

```
tmux new-session -s <SESSION_NAME>
```

In this command, `SESSION_NAME` is a Tmux session name of your choice. For example:

```
tmux new-session -s AADS_session
```

2. To re-connect to the Tmux session, run the following command:

```
tmux attach-session -t <SESSION_NAME>
```

In this command, `SESSION_NAME` is the name of the Tmux session that you created. For example:

```
tmux attach-session -t AADS_session
```

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 Workplace Client softphones 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

UDP

User Datagram Protocol. This is a communication method, similar to TCP.

Index

Special Characters

_Admin user is not prompted for password in sudo su	401
_full disk space	428
_REPLACE THIS TEXT, OR DELETE THIS ENTIRE INDEXTERM ELEMENT IF YOU DO NOT NEED IT	142

Numerics

10.2.0.1	22
10.2.1	22
10.2.1.1	22
10.2.1.4	21

A

AADS 10.2.0.1	22
AADS 10.2.1.4	21
access denied error	400
access token	49
configuring expiry time	149
activate	
firmware package	262
AD FS integration	
configuration checklist	86
adding	
enterprise users to Avaya Spaces	165
LDAP server	184
platform for dynamic configuration	270
trusted host	207
adding users	
to Auth0 for SSO	113
to IBM SVA	101
to OKTA	81
additional base context DN	193
additional seed node	302
address discovery management	38
ADFS	
configuring claim issuance policy	89
configuring Keycloak as relying party trust	88
configuring on Keycloak	88
ADFS integration	
attribute mapping	138
adjusting virtual hardware parameters	413
CPU	415
memory	415
Admin Interface	
enabling Cross-Origin resource sharing	42
administration roles	31
administration tools	
clitool-acs	446
collect decrypted logs	426

administration tools (<i>continued</i>)	
collectlogs	445
statusAADS utility	446
AIDE	
automatic scanning	314
creating baseline database	312
disabling automatic scanning	315
excluding files from scanning	313
manual scanning	314
overview	311
reviewing scan report	316
scanning overview	313
Alarm	428
alarms	
description	342
overview	337
System Manager	338
System Manager does not show Device Services alarms	407
third-party SNMP	340
verify	341
aliases	464
allocate	
disk space to logical volumes	411
antivirus	303
prerequisites	304
setting SELinux permissive mode	304
API key	
creating	155
obtaining	156
API key secret	
obtaining	156
app command	464
appcast item	
deleting	244
editing	243
field descriptions	242
non-interactive upgrade	243
assigning group to IBM SVA application	99
assigning group to OKTA application	82
attribute mapping	
configuring	199
for ADFS identity provider	138
for Auth0 identity provider	141
for Duo identity provider	140
for IBM SVA identity provider	139
for Imprivata identity provider	141
for Microsoft Azure identity provider	136
for Office 365 identity provider	136
for OKTA identity provider	82, 138
for OneLogin identity provider	93, 100, 139
for Ping Identity identity provider	74, 137
overview	47

audit	176	Avaya Spaces (<i>continued</i>)	
Auth0 integration		phone number synchronization	160
checklist	109 , 195	stopping synchronization	159
configuring identity provider on Keycloak	112	time zone file format	163
creating new SSO application	110	trial license	164
creating users	113 , 114	troubleshooting synchronization	425
authentication		unblocking	425
testing	146	updating configuration	179
authentication domain		updating language and time zone settings	161
selecting	202	user audit	176
authentication realm	48	user management	172
Auto Configuration Failure	429	user management overview	163
automatic backups	352 , 353	viewing connection status	181
changing location	354	Avaya Spaces connection	
location changed after upgrade	428	view status	181
automatic configuration service	391	Avaya Spaces integration	
automatic file system scanning		cancelling license upgrade	178
disabling	315	cancelling registration	178
automatic registration	168 , 170	creating API key	155
LDAP group priority	169	deallocating licenses	173
unregistering LDAP group	172	deleting	181
updating settings	171	disabling	180
Avaya Aura Device Services	31	obtaining API key and key secret	156
administration tools	444	registering enterprise users	166
backing up	351	removing Avaya Spaces users	175
entry points	324	removing unregistered enterprise user	167
overview	21	reviewing user information	173
viewing server status	446	selecting enterprise users for registration	165
Avaya Authorization		updating user licenses	174
restricting access	151	Avaya Spaces licenses	
Avaya Breeze		updating license for user	174
importing identity certificate to Avaya Aura Device		Avaya support website	442
Services	37	Avaya Support website	
Avaya InSite Knowledge Base	443	downloading updates	369
Avaya Solutions Platform		Avaya Workplace Client	
migration considerations	367	configuring contact search options	33
Avaya Spaces		displays authentication error	419
audit status	177	download statistics	245
automatic registration of LDAP group users	168	update not working	403
cancelling automatic registration	172	uploading installation files on web deployment	
cannot register enterprise user	424	service	240
configuring account	154	Avaya Workspaces Client cannot connect to Device	
configuring company	154	Services	397
configuring domain	154	Avaya Workspaces for Oceana	
configuring LDAP group automatic registration	202	integration	37
configuring settings on Avaya Aura Device Services	156	AVP	
configuring SSO	182	adjusting parameters	413
configuring synchronization	158	completing upgrade	384
connection errors	422	deploying new virtual machines	383
Device Services does not contain Spaces certificate	423	rolling back upgrade	385
enabling automatic registration	170	upgrading virtual machines	381
Enterprise SSO	155	AVP upgrade	
integration checklist	153	preparing for upgrade	379
integration paramters	179	AWS	297
languages file format	162		
license types	164		
overview	153		

B

back up	
automatic	352, 353
Avaya Aura Device Services deployed on ESXi or AWS	373
overview	351
phone model to group ID mapping	259
phone settings	256
Utility Server	258
backup and restore	351
backups	
changing automatic backup location	354
base context DN	
configuring additional base context DN	193
browser clients	
Device Services does not process requests	427
bulk import	
field descriptions	285
overview	282
supported special characters	283
user data to Open LDAP	211
bulk upload	
CSV file structure	209

C

canceling	
scheduled log collection	336
cancelling	
automatic registration of LDAP group users	172
cancelling user registration on Spaces	
Spaces license upgrade	178
Cassandra	
clustering	298
does not start when reinstalling node	417
re-assigning nodes	300
reviewing status	301
schedule maintenance	43, 299
cdto command	465
certificate	
expiration warning	231
Certificate Policy	401
certificate revocation	233
configuring	235
System Manager certificates	404
certificate signing request	
parameter description	229
certificates	
browser clients	427
importing Avaya Breeze authorization certificate	37
obtaining latest Avaya Spaces certificate	423
System Manager	399
third party CA signed certificates	236
changes to platform support	17
changing	
CPU and memory resources	415

changing (<i>continued</i>)	
Keycloak password	123
characters in passwords	323
checking	
Avaya Aura Device Services status	327, 447
DRS synchronization	393
checklist	
AD FS provider configuration	86
Auth0 identity provider configuration	109, 195
Duo provider configuration	102
IBM SVA provider configuration	95
Imprivata provider configuration	106
integration with Avaya Spaces	153
Microsoft Azure identity provider configuration	58
Office 365 OAuth identity provider configuration	64
OneLogin provider configuration	90
Ping Identity provider configuration	70, 76
SSO device flow	115
system layer update	368
upgrading Device Services	218, 366, 436
Workspaces SSO Flow	119
client certificate policy	35
Client login failure when Identity provider link already exists in Keycloak	432
client mapping	
creating	126
creating for	116
creating for Workspaces SSO Flow	119
public key update interval	129
regenerating client secret	129
client secret	
obtaining	67
clients	
uploading Avaya Workplace Client installation files	240
clitool-acs utility	446
cluster	
enabling LDAP replication	391
enabling OAuth database replication	151
restoring	360
cluster nodes	
field descriptions	326
collect	
logs	336
collection	
delete	440
edit	440
generating PDF	440
sharing content	440
command values	
Windows Domain Controller	293
commands	
system layer	448
complexity rules for passwords	323
components	25
Avaya Aura Device Services	25
configuration	
active directory	291

configuration (<i>continued</i>)			
automatic configuration flow	24	contact search (<i>continued</i>)	
exporting configuration file	357	restricted search	212
field descriptions	271	restricting search	215
IWA	290, 291	restricting search to user's group	214
setting	273	content	
Windows Domain Controller	291	publishing PDF output	440
Workspaces SSO Flow	118	searching	440
configuration file		sharing	440
OKTA identity provider	79	sort by last updated	440
Ping Identity identity provider	72	watching for updates	440
configuration parameters		CORS configuration	
Avaya Aura Device Services specific parameters	274	cross-origin resource sharing	41
configuration portability	356	creating	
exporting configuration file	356	baseline database for AIDE scanning	312
updating configuration file	358	client mapping	126
configuring		new application for SSO on Auth0	110
additional seed node	302	new application for SSO on Microsoft Azure	59
automatic backup	353	new configuration	271
automatic file system scanning	314	cross-side request forgery attacks	321
automatic registration of users on Spaces	170	CSR	
Avaya Spaces account	154	connecting Avaya Aura Device Services to Avaya	
Avaya Spaces integration	156	Aura Web Gateway	228
certificate expiration warning	231	create	227
certificate revocation settings	235	custom files	
client certificate policy for REST	35	accessing	255
contact search	33	uploading on Utility Server	254
data encryption	306	viewing	255
data retention period	303		
domain user properties in FIPS mode	293	D	
expiry time for access and refresh tokens	149	data encryption	
Keycloak for OAuth	124	collecting encrypted logs	426
LDAP attribute mapping	199	disabling remote key server	308, 309
LDAP UID mapping for SSO integration	144	enabling remote key server	307
LDAP user deletion warning	205	encryptionPassPhrase command	460
log retention period	303	local key store	311
logging in to Avaya clients	285	overview	27, 306
network settings	220	passphrase	308
OAuth database replication	151	remote key server	307
password rules	458	removing passphrase	309
remote logging	332	reviewing passphrase status	310
RSA public and private keys	387	viewing status	310
samesite cookie	321	data encryption commands	460
secure boot	320	encryptionRemoteKey	461
software update deployment	240	encryptionStatus	461
SSH connections	387	data replication	391
TLS	319	data retention	27, 303
windows authentication	200	database repair	43, 299
configuring network settings		deactivate	
prerequisites	219	firmware package	263
configuring password rules	324	deallocating	
connection check errors	422	Avaya Spaces licenses	173
contact integrity logs disabled	407	default identity provider	132
contact search		disabling	133
disabling	215	deleting	
enabling LDAP	213	appcast item	244
in additional Base DNs	213	Avaya Spaces integration	181

deleting (<i>continued</i>)		DRS (<i>continued</i>)	
Avaya Spaces users	175	repairing state	398
deploy		troubleshooting	398
new AVP virtual machine	383	Duo	
deployment options	28	adding application to Duo Access Gateway	104
descriptions		configuring on Keycloak	105
certificate assignment	232	configuring SAML application	103
device authorization flow	51	Duo integration	
checklist	115	attribute mapping	140
configuration	115	configuration checklist	102
J100 parameters	118	dynamic configuration	
prerequisites	54	adding platforms	270
Device Authorization Flow		Avaya Aura Device Services specific parameters	274
client mapping	116	configuring automatic log in to Avaya clients	285
DHCP server	249	creating new configuration	271
diagram		default field descriptions	287
automatic configuration flow	24	default settings	286
solution architecture	23	deleting platforms	270
directory		priorities	268
excluding from AIDE scanning	313	dynamic configuration service	38
disabling		overview	265
Avaya Spaces integration	180	dynamic configuration settings	
contact search	215	assigning group identifiers to phone models	269
identity provider	121	implementation	268
identity provider redirector	68	importing	279
local key store	311	JSON file example	280
remote key server	308 , 309	password masking	273
STIG hardening	317	updating default settings	286
Disabling			
PhoneBackup Feature or Whitelist Custom IP Range	257	E	
discovering LDAP using SRV records	196	EASG	
disk encryption		enabling from CLI	349
disabling	306	removing	350
enabling	306	editing	
passphrase complexity rules	309	appcast item	243
disk size		SSO client mapping	128
increasing ESXi VM disk size	413	enableVantageFWSupport.sh	463
DNS		enabling	
server addresses disappear	402	Avaya Spaces integration	156
DNS SRV records for LDAP	196	Cross-Origin resource sharing for Admin Interface	42
document changes	18	Cross-Origin resource sharing for Service Interface	41
documentation center	440	EASG	349
finding content	440	LDAP authentication for OAuth	199
navigation	440	remote key server	307
documentation portal	440	scheduled log collection	335
domain user		single-user mode	430
configuring	293	Split Horizon DNS mapping	289
download		STIG hardening	317
logs	336	encryptionPassphrase	460
downloading		encryptionRemoteKey	461
Avaya Workplace Client from web deployment		encryptionStatus	461
service	240	endpoints	
system layer update	369	firmware upgrade is not working	409
DRS		supported by Utility Server	247
fails with constraint error	399	uploading firmware upgrade file to Utility Server	252
not polling	398	uploading settings file to Utility Server	253
ready to repair	398		

enterprise directory attribute mappings	
modifying	199
Enterprise LDAP server configuration	
field descriptions	186
Enterprise SSO	155
enterprise users	
cancelling registration process	178
registering on Avaya Spaces	166
reviewing information	173
selecting for registration on Avaya Spaces	165
entry points	324
ESG	401
ESXi	
increasing virtual disk size	413
excluding	
files from AIDE scanning	313
exit	
single-user mode	432
exporting configuration data	356
exporting configuration file	
from administration portal	356
from CLI	357
external load balancer	
enabling	34
F	
Feature Configuration	
PhoneBackup	257
field descriptions	
application properties	32
file	
excluding from AIDE scanning	313
file system	
automatic scanning	314
creating baseline database	312
manual scanning	314
finding content on documentation center	440
FIPS	
configuring domain user properties	293
firmware	
updating path to 46xxsetting.txt file in upgrade file	262
upgrade is not working	409
firmware management	259
firmware package	
activating	262
firmware package	260 , 463
deactivating	263
increasing size limit	252
removing from Utility Server	264
statuses	260
unpacking	261
firmware packages	
checking free space on Utility Server	251
firmware upgrade file	
uploading to Utility Server	252
flows	

flows (<i>continued</i>)	
request flow	46
response flow	46

H

health check	328
enabling HTTPS	329 , 463
HTTP Proxy	325
HTTPS	
for node health checks	329 , 463
human-user accounts	
configuring password rules	324

I

IBM SVA	
adding users to groups	101
assigning group to application	99
configuring on Keycloak	98
configuring Populations group	98
configuring SAML application	96
creating users	101
IBM SVA integration	
attribute mapping	139
configuration checklist	95
identity certificate	
expiration warning	231
identity provider	
attribute mapping for ADFS	138
attribute mapping for Auth0	141
attribute mapping for Duo	140
attribute mapping for IBM SVA	139
attribute mapping for Microsoft Azure	136
attribute mapping for Office 365 OAuth2	136
attribute mapping for OKTA	138
attribute mapping for OneLogin	139
attribute mapping for Ping Identity SAML v2.0	137
configuring Duo application	103
configuring IBM SVA application	96
configuring OKTA application	78
configuring OneLogin application	92
configuring Ping Identity application	71
default provider	132
disable	121
error page is displayed to user	418
importing third-party provider	131
Imprivata attribute mapping	141
interoperability issues	421
mapping Keycloak attributes	133
switching	120 , 121
user cannot log in	418
user cannot reach login page	417
identity provider integration	
testing using web browser	146
identity providers	
simultaneous use	50

importing		Keycloak (<i>continued</i>)	
46xxsettings file	282	configuring Auth0 identity provider	112
bulk configuration setting	284	configuring Microsoft Azure identity provider	63
dynamic configuration settings	279	creating client mapping	126
dynamic configuration settings using JSON file	280	default identity provider	132
keystore data	230	deleting users	121
Importing Certificate	143	downloading identity provider settings	108
importing configuration data	356	Duo SAML checklist	102
importing users to Open LDAP	209	editing client mapping	130
Imprivata		IBM SVA SAML checklist	95
attribute mapping	141	importing identity provider private CA certificates	130
configuring LDAP settings	107	importing third-party identity provider	131
configuring on Keycloak	108	Imprivata checklist	106
Imprivata integration		logs	152
configuration checklist	106	mapping identity provider attributes	133
Imrpivata		Microsoft Azure SAML checklist	58
role fetching	107	obtaining client secret	126
inaccessible resources	427	Office 365 OAuth2 checklist	64
increase		OneLogin SAML checklist	90
disk size	413	Ping Identity SAML checklist	70, 76
increasing the size		realm configuration for UC servers	123
disk volume	415	regenerating client secret	129
initializing		starting and stopping	126
baseline database for AIDE scanning	312	troubleshooting	417
installation		web administration portal	122
fails	399	Keycloak configuration	144
installing		Keycloak Truststore	143
staged system layer update	370	keystore	
Integrated Windows authentication support setup	290	importing keystore data	230
IP phone firmware		keystore data	
available disk space	247	managing	230
IWA			
active directory	291	L	
administration portal	294	LDAP	144, 429
prerequisites	290	disabling contact search	215
Windows Domain Controller setup	291	discovery using DNS SRV records	196
J		enabling LDAP authentication for OAuth	199
J100		enabling search	213
publishing settings for SSO	118	Open LDAP operations	209
JSON file		settings for Imprivata IDP	107
for importing configuration settings	280	stopping synchronization	203
K		supported characters	208
KB		testing connection	197
Support site	443	updating user attributes	208
Keycloak		user deletion policy	204
AD FS SAML checklist	86	LDAP configuration	
adding hard-coded user role	68, 69	Active Directory internationalization parameters	206
attribute mapping overview	47	additional base context DN	193
Auth0 SAML checklist	109, 195	attribute mapping	199
blocking access to Avaya Authorization	151	configuring photoURI attribute	211
changing password	123	importing secure LDAP certificate	235
checklist	55	provenance priority	198
configuring	124	selecting authentication domain	202
		LDAP server	
		adding	184
		configuration	198

LDAP server (<i>continued</i>)		
discovery options	194	
user synchronization	202	
user synchronization after deployment	394	
user synchronization fails	409	
LDAP server certificate	142	
LDAP server management		
overview	40 , 183	
LDAP user deletion warning		
disabling	205 , 206	
license		
cancelling Spaces license upgrade	178	
cannot deallocate license from Avaya Spaces user ...	425	
licensecannot delete Avaya Spaces user		
cannot update license for Avaya Spaces user	425	
licenses		
Avaya Spaces user license types	164	
Avaya Spaces user licenses management	172	
deallocating Avaya Spaces licenses	173	
linux		
single-user mode	430	
load balancer		
enabling external load balancer	34	
local key store		
disabling	311	
enable	311	
Locate		
keystore password	355	
log management		
canceling scheduled log collection	336	
configuring log retention	303	
Keycloak logs	152	
overview	332	
remote logging	332	
scheduling log collection	335	
logging in to		
Avaya Aura Device Services administration portal	30	
Utility Server	250	
logical volumes		
allocating unused disk space	411	
login mechanisms	324	
logs		
collecting encrypted logs from command line		
interface	426	
collecting logs from command line interface	445	
downloading	336	
setting up Avaya Aura Device Services log level	334	
M		
managing		
application sessions	32	
Avaya Spaces users	172	
CSRs	227	
firmware on Utility Server	259	
identity certificates	226	
keystore data	230	
managing (<i>continued</i>)		
server interface certificates	232	
System Manager certificates	225	
truststore certificates	233	
managing certificates		
web administration portal	35 , 225	
mapping		
IP address to FQDN	288	
messaging server		
server address discovery	38	
Microsoft Azure		
assigning users to SSO application	62	
configuring user groups	61	
obtaining group ID	62	
Microsoft Azure integration		
checklist	58	
configuring settings on Keycloak	63	
creating new SSO application	59	
migrating	365	
migrating AADS	435	
Migrating to KVM	435	
migration		
Avaya Solutions Platform	367	
modifying		
provenance priority	198	
monitor		
Avaya Aura Device Services logs	333	
monitoring		
cluster nodes	326	
remote node	328	
multiple authentication domains		
configuring uid	184	
multiple domains		
selecting authentication domain	202	
N		
network parameters configuration		
post-requirement	221	
network settings		
updating	220	
network settings configuration	217	
new in release	21 , 22	
new in this release		
Release 10.2	23	
new private key		
failed to generate	401	
non-Aura deployment	28	
SIP client considerations	267	
non-interactive upgrade for Windows clients	243	
note		
VM configuration details	436	
O		
OAuth		
configuring expiry time for tokens	149	

OAuth (<i>continued</i>)		operating system (<i>continued</i>)	
configuring Keycloak	124	updating	368
enabling database replication	151	updating system layer	371
Keycloak administration portal	44	overview	
LDAP authentication	199	Avaya Aura Device Services	21
web administration portal	122	overwriting	
OAuth integration		existing configuration	275
configuring LDAP UID mapping	144		
OAuth2		P	
concepts	44	passphrase	
troubleshooting	417	reviewing status	310
obtaining		passphrase	
client secret for Office 365 OAuth2 integration	67	complexity rules	309
group ID on Microsoft Azure	62	remove	309
Office 365 integration	64	password	
attribute mapping	136	changing Keycloak password	123
checklist for Office 365 OAuth2 configuration	64	single-user mode	431
creating hard-coded user role	68 , 69	password complexity rules	323
disabling identity provider redirector	68	password masking	273
enabling read permissions for application	66	password rules	
OAuth2 integration	65	configuring	324 , 458
obtaining application client secret	67	supported characters	323
obtaining application ID	66	performance	
registering application on Azure portal	65	charts overview	330
OKTA		slow performance	403
adding users to groups	81	viewing statistics	329
assigning group to application	82	performing a backup	351
configuring attribute mapping on OKTA	82	automatic	353
configuring on Keycloak	79	phone custom files	
configuring Populations group	80	accessing	255
configuring SAML application	78	uploading on Utility Server	254
creating users	81	phone firmware package	
obtaining configuration file	79	increasing size limit	252
OKTA integration		phone model to group ID mapping	
attribute mapping	138	backup	259
OneLogin		restore	259
adding users		phone models	
to OneLogin	94	supported by Utility Server	247
configuring on Keycloak	93	phone numbers synchronization	160
configuring SAML application	92	phone settings	
creating users	94	backing up	256
OneLogin integration		Ping Identity	
attribute mapping	139	adding users	
configuration checklist	90	to Ping Identity	76
Open LDAP		configuring on Keycloak	75
configuring photoURI attribute	211	configuring Populations group	73
CSV file structure	209	configuring SAML application	71
replication	392	creating users	76
uploading users	209 , 211	obtaining configuration file	72
Open LDAP replication		Ping Identity integration	
replication is failed	410	attribute mapping	137
TLS negotiation failure error	410	configuration checklist	70 , 76
OpenLDAP		platforms	
enabling data replication	391	adding	270
operating system		deleting	270
single-user mode	430	port	
update checklist	368		

port (<i>continued</i>)		restore (<i>continued</i>)	
Web Deployment	239	Utility Server data	259
ports		restoring	
SNMP	340	cluster	360
PPM certificate error	405	standalone system	358
prerequisites		retrieving	
for antivirus installation	304	configuration settings	279
for device authorization flow configuration	54	Retrieving	
for SAML v2.0/OAuth2 SSO configuration	52	Cassandra database username and password	355
for SSO configuration	52	reviewing	
for Workspaces SSO configuration	54	AIDE scan report	316
IWA	290	Avaya Spaces users	173
network settings configuration	219	data encryption status	461
Presence Services		revocation	
server address discovery	38	certificates	235
primary node	405	roll back	
private key		AVP upgrade	385
failed to generate	401	upgrade	376
processing CA signing requests	229	Rolling	
provenance priority		Back Changes	258
modifying	198	root access	305
public keys		RSA public and private keys	387
update interval	129	runUserDiagnostics	462
published settings	278		
publishing		S	
configuration settings	276	samesite cookie	321
		web-based clients	322
R		SAML identity provider	
reconnecting to System Manager	404	for Auth0	112
refresh token	49	for Microsoft Azure	63
configuring expiry time	149	SAML v2.0/OAuth2 SSO	
regenerating client secret	129	prerequisites	52
registering enterprise users		scanning	
cancelling registration	178	automatic file system scanning	314
registering enterprise users on Spaces	166	disabling automatic file system scanning	315
registration		manual file system scanning	314
automatic registration of users on Spaces	168	scheduled log collection	335
reinstall		canceling	336
cannot reinstall non-seed node	417	scheduling	
related documentation	439	Cassandra database maintenance	43, 299
remote key server	307	search	
disable	308, 309	contact search	212, 215
enable	307	contact search in user's group	214
remote logging	332	enable contact search for LDAP	213
removing		searching for contacts	
EASG	350	configuring for Avaya Workplace Client	33
firmware package from the Utility Server	264	searching for content	440
repairing faulty users	406	secure boot	320
request flow	46	checking status	320
resolv.conf		secure connection	233
does not contain DNS addresses	402	secure LDAP certificate	
response flow	46	importing using web administration portal	235
REST API		Secured LDAP user federation with keycloak error	
SSO for Avaya Spaces Clients	182	occurs during configuration settings	433
restore		security	
phone model to group ID mapping	259	log retention period	303

seed node		Spaces (<i>continued</i>)	
cannot access resources	427	connection errors	422
configuring additional seed node	302	integration checklist	153
selecting		license types	164
authentication domain	202	overview	153
logging level	334	stopping synchronization	159
SELinux		trial license	164
permissive mode	304	troubleshooting synchronization	425
server address and credentials		unblocking	425
field descriptions	186	user management	172
Service Interface		user management overview	163
enabling Cross-Origin resource sharing	41	viewing connection status	181
serviceability agents	338	Spaces integration	
setting		creating API key	155
company domain	154	deallocating licenses	173
setting up		deleting	181
Avaya Spaces integration	156	deleting Avaya Spaces users	175
DHCP server for Utility Server	249	disabling	180
IWA	294	obtaining API key and key secret	156
user synchronization	202	registering enterprise users	166
user synchronization after deployment	394	removing unregistered enterprise user	167
settings		reviewing user information	173
user, group, global, platform, and exception	273	selecting enterprise users for registration	165
settings file		updating user licenses	174
Avaya Aura Device Services specific parameters	274	Spaces licenses	
uploading to Utility Server	253	updating license for user	174
sharing content	440	special characters	
shutting down		for dynamic configuration settings	283
Avaya Aura Device Services	447	for LDAP attributes	208
silent installation		Split Horizon DNS mapping	
exporting configuration file	356 , 357	enabling	289
single sign-on		field descriptions	289
enabling OAuth database replication	151	mapping IP address to FQDN	288
single-user mode	430	overview	288
exiting	432	SPSSODescription file	108
logging in	430	SSH connections	
SIP parameters		cluster	387
non-Aura deployments	267	SSH timeout	466
SNMP	337 , 338 , 340	SSH/RSA keys	
installation	340	cannot generate new private key	401
Send to a third-party server	341	SSO	44
verify	341	access and refresh tokens	49
SNMP target profile		authentication fails	420
setting up	339	authorization flow	46
SNMPv3 user profile		device authorization checklist	115
assigning	339	device authorization flow	51
setting up	338	editing client mapping	128
software-only		for Avaya Spaces	182
system layer upgrade	371	J100 parameters	118
solution topology	23	prerequisites	52
sort documents	440	synchronize with identity providers	145
Spaces		Workspaces Flow checklist	119
configuring account	154	SSO authentication	
configuring company	154	token realm	48
configuring domain	154	SSO integration	
configuring settings on Avaya Aura Device Services	156	configuring LDAP UID mapping	144
configuring synchronization	158	staged system layer	

staged system layer (<i>continued</i>)		testing (<i>continued</i>)	
installing	370	configuration settings	276
staging system layer	369	integration with identity provider	146
standalone system		OAuth2 configuration testing results	148
restoring	358	SSO configuration	147
start	31	timeout	466
starting		TLS	318
Keycloak service	126	configuring	319
Utility Server	249	TLS negotiation failure	410
status		tmux	466
checking	327 , 447	token realm	48
statusAADS command		trial Avaya Spaces licenses	164
usage	446	troubleshooting	400 , 407
STIG hardening		cannot access resources	427
disabling additional hardening options	317	cannot register enterprise user on Avaya Spaces	424
enabling	317	cannot upload large firmware	409
stopping		DNS entries in resolv.conf	402
Keycloak service	126	DRS	398
Utility Server	249	error page is displayed	418
support	442	expired Avaya Spaces certificates	423
supported		identity provider interoperability issues	421
antiviruses	303	interaction with browser clients	427
synchronization with LDAP server fails	409	logs are encrypted	426
synchronizing		OAuth2	417
Avaya Spaces user data	158	recovering synchronization	425
Avaya Spaces user information	176	repairing Cassandra clustering	429
phone numbers in LDAP and Avaya Spaces	160	Spaces pages blocked	425
Synchronizing		SSO authentication fails	420
client ID	364	synchronization with LDAP server fails	409
sys	448	System Manager certificates	399
sys ipv6config	457	user cannot log in	418
sys secconfig	449	user cannot log in to identity provider	420
sys smcvemgt	454	user cannot reach login page	417
examples	457	verifying attributes imported for user	419
sys versions	450	verifying that attributes are imported correctly	420
sys volmgt	450	Workplace Client displays authentication error	419
system layer		truststore	
commands	448	does not contain Avaya Spaces certificate	423
ipv6config	457		
secconfig	449	U	
smcvemgt	454 , 457	UEFI	320
update checklist	368	UEFI secure boot	
updating	368	checking status	320
updating for software-only	371	unpack	
versions	450	firmware package	261
volmgt	450	update	
system layer update		system layer (OS)	368
downloading	369	system layer for software-only deployments	371
System Manager		update error	
primary System Manager fails	403	Avaya Workplace Client	403
reconnecting after reinstalling certificates	404	updating	
System Manager certificates	399	default dynamic configuration parameters	286
system update	368	network settings	220
		user attributes in LDAP	208
T		updating an existing stack	
testing		CloudFormation template	297

upgrade		
Avaya Aura Device Services	372 , 373	
Avaya Aura Device Services deployed on AVP	377	
AVP virtual machines	381	
expired Avaya Spaces certificates	423	
location of automatic backups changed	428	
preparing for AVP upgrade	379	
rolling back	376	
rolling back AVP upgrade	385	
upgrade file		
update path to 46xxsettings.txt file	262	
upgradeAutoConfigTestConfigurations	389	
upgrading	365	
ESXi	367	
installing system layer updates	370	
test configurations	389	
upgrading Device Services		
checklist	218 , 366 , 436	
uploading		
Avaya Workplace Client	240	
files on Utility Server	252	
phone custom files on Utility Server	254	
upgradingOVA- based virtual machines	395	
upgradingRHEL 8.4 to RHEL 8.10	395	
user		
cannot cannot log in to identity provider	418	
cannot reach login page of identity provider	417	
error page is displayed	418	
user data retention	27	
user role mapping		
fetch roles from LDAP	107	
Users cannot log in to the client due to expiry of third-party identity provider certificate	434	
utility server		
enabling HTTP access	250	
overview	246	
supported browsers	246	
uploading firmware upgrade file	252	
uploading settings file	253	
Utility Server		
activating firmware	262	
backing up	258	
backing up phone settings	256	
cannot upload large firmware	409	
capacity	247	
deactivating firmware	263	
firmware management	259	
firmware package	260	
firmware package size limit	463	
firmware upgrade is not working	409	
increasing firmware package size limit	252	
logging in	250	
migrating data	388	
removing firmware	264	
restoring data	259	
setting up a DHCP server	249	
starting	249	
Utility Server (<i>continued</i>)		
stopping	249	
supported phone models	247	
unpacking firmware	261	
updating path to 46xxsettings.txt file	262	
uploading files	252	
uploading phone custom files	254	
viewing IP phone custom files	255	
V		
Vantage		
firmware package size limit	463	
increasing firmware package size limit	252	
Vantage firmware package		
cannot upload to Utility Server	409	
verifying		
company domain address	154	
Verifying		
configuration status of PhoneBackup	258	
videos	442	
view published settings	278	
viewing		
Avaya Spaces connection status	181	
data encryption status	310	
home location	268	
viewing performance data	329	
charts overview	330	
virtual hardware		
adjusting CPU resources	415	
adjusting memory resources	415	
adjustments	413	
VMware		
adjusting CPU and memory resources	415	
VMware to KVM		
preparing for migration	437	
W		
watchlist	440	
web administration portal	405	
Keycloak	122	
not accessible	405	
web deployment		
Avaya Workplace Client download statistics	245	
Web Deployment		
port configuration	239	
web deployment service		
Avaya Workplace Client download statistics	245	
uploading Avaya Workplace Client	240	
Web Deployment service		
interactive and non-interactive client upgrade	243	
overview	43 , 239	
web portal administration roles	31	
web-based clients		
configuring samesite cookie	322	
Windows authentication		

Windows authentication (<i>continued</i>)	
configuring	200
Workspaces SSO	
prerequisites	54
Workspaces SSO Flow	
checklist	119
client mapping	119
configuration	118