# Administering Avaya Aura® Device Services

Release 7.0.1
Issue 2
January 2017

**Notice**

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

**Documentation disclaimer**

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

**Link disclaimer**

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

**Warranty**

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

**Hosted Service**

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

**Licenses**

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

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

**License types**

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

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

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

**Copyright**

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

written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

**Virtualization**

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

**Third Party Components**

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

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

**Service Provider**

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

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

**Compliance with Laws**

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

**Preventing Toll Fraud**

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

**Avaya Toll Fraud intervention**

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

**Security Vulnerabilities**

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

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

**Downloading Documentation**

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

**Contact Avaya Support**

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

**Trademarks**

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

Avaya is a registered trademark of Avaya Inc.

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

# Contents

# Chapter 1: Introduction

## Purpose

This document contains information about how to perform Avaya Aura® Device Services administration tasks including how to use management tools, how the manage data and security, an how to perform periodic maintenance tasks.

This document is intended for people who perform Avaya Aura® Device Services system administration tasks such as backing up and restoring data and managing users.

# Chapter 2: Avaya Aura® Device Services overview

Avaya Aura® Device Services provides a set of services to Avaya Equinox™ 3.0. Avaya Aura® Device Services is co-resident with Session Manager and is delivered as separate OVA.

The following services are provided when using Avaya Aura® Device Services with Avaya Equinox™ 3.0:

- **Contact:** To use the Contact service, a user must be a provisioned user on LDAP Server. Using the contact service, you can:
  - Manage the contact detail from any device.
  - Add, update, and delete a contact.
  - Perform an enterprise search of existing sources of contacts, such as, System Manager, multiple LDAPs, single LDAP multiple domains, and local only.

    Avaya Aura® Device Services supports directory search of up to 300 contacts. The number of contacts displayed in search results for a client depends on the number of search results that the client supports.
  - Set and retrieve information, such as, preferred names, picture, and preferences. Using the Picture service, you can create and override, delete, and update the picture of a user. This also provides a centralized, firewall-friendly interface to include these picture urls in the contact information or search results.
  - Search and retrieve information about Avaya Scopia® users and terminals.

    You can use Avaya Aura® Device Services to search for Avaya Scopia® users and terminals only when iView's address is configured on Avaya Aura® Device Services.
- **Notification:** The Notification service provides a common infrastructure that allows a client or endpoint to subscribe to receive events from a number of service resources using a single connection.
- **Dynamic Configuration:** The Dynamic Configuration service provides discovery of configuration settings to UC Clients. You can customize these settings on a global, group, individual, or platform basis. The Dynamic Configuration service uses the automatic configuration feature of Avaya Equinox™ 3.0 to facilitate the configuration details to the UC clients. This helps the user to avoid manual configuration of their client. To log in to the client, the user needs to enter their credentials, such as, email address or Windows user id, along with their enterprise credentials.

The Dynamic Configuration service is supported on the following Avaya Equinox™ 3.0 devices:

- Avaya Equinox™ for Android
- Avaya Equinox™ for iOS
- Avaya Equinox™ for Mac
- Avaya Equinox™ for Windows

- **Web Deployment:** The Web Deployment service publishes and deploys the UC client updates to the devices of the end users. The Web Deployment service is supported on the following devices of the Avaya Equinox™ 3.0:
  - Avaya Equinox™ for Mac
  - Avaya Equinox™ for Windows

# Chapter 3: Management tools

## Logging in to the Avaya Aura® Device Services web interface

### About this task

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

### Procedure

1. Open a compatible web browser.
2. Type the URL in one of the following formats:
   - `https://<IP_Address>:8445/admin/`
   - `https://<FQDN>:8445/admin/`

   For using FQDN, you must add the IP address and FQDN of Avaya Aura® Device Services in the etc/hosts file of the system from where you are accessing the Avaya Aura® Device Services web interface. The default path of the hosts file on a Microsoft Windows system is `C:\Windows\System32\drivers\etc`.
3. Press `Enter`.

   If your browser does not have a valid security certificate, the system displays a warning with instructions to load the security certificate.
4. **(Optional)** If you are certain your connection is secure, accept the server security certificate to access the Logon screen.
5. On the Logon screen, do the following:
   a. In the **Username** field, type the user name.
   b. In the **Password** field, type the password.

   To access the web-based administration portal, use an account with an administrator role defined in the LDAP server configuration.
6. In the **Password** field, type the password.
7. Click **Log on**.

   The system displays the Avaya Aura® Device Services home page.

# 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 (aka 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, collectLogs, and collectNodes.
  - clitool-acs

    A tool that has multiple usage possibilities. The parameters specified in the command determine the usage of the clitool-acs utility.
  - collectLogs

    Copies the logs from an Avaya Aura® Device Services node to a file or to a directory specified as parameters in the command.
  - collectNodes

    Copies the logs from all the nodes in an Avaya Aura® Device Services cluster to the file specified in the command.
  - 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 adapter is enabled and available.

- wget

  Downloads files from the Web.

  You can use this tool to perform resource discovery for a user.

- curl

  Transfers a URL.

---

# clitool-acs

The clitool-acs utility provides multiple usage possibilities, depending on which parameters the utility receives in the command line.

## Usage example

Run the clitool-acs.sh utility with the appropriate parameters. To view the command options, run the clitool-acs.sh utiltity without any parameters.

For example:

```
[admin@aads-dev-114 ~]$ sudo /opt/Avaya/DeviceServices/7.0.1.0.2804/CAS/7.0.1.0.2804/misc/
clitool-acs.sh
Usage:
clitool-acs.sh listClusterNodes
clitool-acs.sh applicationInterface <start|stop>
clitool-acs.sh removeClusterNode <serverUUID> [force]
clitool-acs.sh clusterVirtualIp [<virtual IP address> master|backup]|[clear <node IP
address>]
clitool-acs.sh systemManagerUPM [<recommended System Manager UPM user and password>]
clitool-acs.sh pushKeytab
clitool-acs.sh registerClusterNode <serverUUID> <IP address> [force]
clitool-acs.sh longpollTimeout [<longpoll timeout duration>]
clitool-acs.sh ldapConfiguration [<ldap properties filename> <ldap user's password>] | --
current
clitool-acs.sh corsConfiguration [<cors propeties filename>]
clitool-acs.sh certWarningPeriod [<number of days>]
clitool-acs.sh notificationFrontend [http|websocket|schemeHTTP|schemeWebsocket|host|port|
<schemeWSS> <schemeHTTP> <host IP or name> <port>
clitool-acs.sh checkVersions
clitool-acs.sh clientCertificateVerificationConfig [<service_name> <off|optional|on>]
clitool-acs.sh restFrontend [scheme|host|port|<scheme> <host IP or name> <port>]
clitool-acs.sh licenseServerUrl <ip/fqdn> <port>
clitool-acs.sh drsSyncDuration [<recommended DRS sync duration timeout>]
clitool-acs.sh microsoftExchangeServer [<recommended Microsoft Exchange Server Details>]
```

## collectLogs

The **collectLogs** utility copies the logs from an Avaya Aura® Device Services node to a file or to a directory specified as parameters in the command.

### Usage example

- **$ sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/bin/collectLogs.sh -n 2 archive_file**: creates an archive called `archive_file.tar.gz` with each of the log files to a count of two, under the current working directory. The two log files are AADS.log and AADS.log.1.

  To create the file in a different directory, add the path to the archive file as a prefix to the file name.
- **$ sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/bin/collectLogs.sh -d /tmp/ -n 2**: copies the log files to the `/tmp` directory with each of the log files to a count of two.
- **$ sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/bin/collectLogs.sh -d /tmp/ -n 2 archive_file**: copies the log files to the `/tmp` directory with each of the log files to a count of two. The -d parameter overrides the current `archive_file` and the `archive_file` is ignored.

## collectNodes

The collectNodes.sh utility creates an archive with logs collected from the Avaya Aura® Device Services cluster nodes.

The archive is created in the current working directory.

**Warning:**

Numerous log files from multiple cluster nodes can occupy a high amount of disk space. Before running the command, ensure that the current node has enough free space.

### Usage examples

$ sudo ./collectNodes.sh [-n <no_of_logs> ] [h] <archive_name>

For example:

```
$ sudo ./collectNodes.sh -n 2 archive_file
```

Creates an archive called archive_file.tar.gz with each of the log files to a count of two, under the current working directory. The two log files are AADS.log and AADS.log.1. To create the file in a different directory, add the path to the archive file as a prefix to the file name

## statusAADS

The statusAADS.sh utility displays the status of the Avaya Aura® Device Services server and of the related services.

### Usage example

Run the statusAADS.sh script from `/opt/Avaya/DeviceServices/<version>/CAS/<version>/bin`.

```
[avaya@AWSDev-14 /]$ sudo /opt/Avaya/DeviceServices/7.0.1.0.1251/CAS/7.0.1.0.1251/bin/
statusAADS.sh
[sudo] password for avaya:
2016-06-23_11:00:04 Displaying status for Avaya Aura Device Services Application
2016-06-23_11:00:04 ulimit file count ..................  [  OK  ]
2016-06-23_11:00:04 ulimit process count ..............  [  OK  ]
2016-06-23_11:00:04 iptables status ....................  [  OK  ]
2016-06-23_11:00:04 RecoveryManager Watchdog status .....  [  OK  ]
2016-06-23_11:00:04 RecoveryManager Service status ......  [  OK  ]
2016-06-23_11:00:05 net-SNMP status ....................  [  OK  ]
2016-06-23_11:00:05 RecoveryManager status .............  [  OK  ]
2016-06-23_11:00:05 AADSKeepalived status ................ [INACTIVE]
2016-06-23_11:00:05 AADSTomcat status .....................  [  OK  ]
2016-06-23_11:00:05 AADSNginx status ......................  [  OK  ]
```

# Chapter 4: Enterprise LDAP Server configuration

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

## Creating groups in LDAP

### About this task

The procedure to create groups might differ depending on the type of enterprise directory used. You must refer the documentation for your enterprise directory to create groups. This section describes the steps for creating LDAP groups in Active Directory.

### Procedure

1. Access Active Directory.
2. Click the **roles** organizational unit.
3. Click the Create Group icon.
4. In the **Group name** field, type the group name and click **OK**.

   You must create the following groups in the enterprise directory that you use:

   - AADSAdmin
   - AADSAuditor
   - AADSUsers
   - AADSServiceAdmin
   - AADSServiceMaintenance
5. To add a user to the group, right-click the user and click **Add to a group**.
6. In the **Enter the object names to select** field, type the group name, and click **OK**.

# Adding a new enterprise LDAP Server

### Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   The system displays the Enterprise LDAP Server Configuration page.
3. Click the plus (+) icon.

   The system displays New Directory tab.
4. In the **Enterprise-Directory Type** field, click the LDAP Server directory that you want to add.
5. In the **Provenance Priority** field, click **Modify**.

   The system displays the Source Provenance Priority pop-up window.
6. In the **Provenance Priority** column, type the priority of the enterprise LDAP Server directory.
7. In the Confirm Action pop-up window, click **OK**.
8. In the Server Address and Credentials section, specify the parameters of the enterprise LDAP Server directory.
9. Click **Save**.

### Related links

Enterprise LDAP Server Configuration field descriptions on page 16

# Enterprise LDAP Server Configuration field descriptions

New Directory

| Name | Description |
|---|---|
| **Enterprise-Directory Type** | Specifies the name of the enterprise directory.<br>The options are:<br>• ActiveDirectory_2008<br>• ActiveDirectory_2012<br>• Novell 8.8<br>• Domino 8.5.3<br>• LDS_2012<br>• LDS_2008<br>• OpenLDAP 2.4.31 |

| Name | Description |
|---|---|
| | • OracleDirectoryServer 5.2 |
| **Provenance Priority** | Specifies the provenance priority of the enterprise directory.<br>Provenance priority is used while merging contacts. If a value is available in more than one directory, the value in the directory with higher provenance priority is returned. For example, if firstName is obtained from two directories, the firstName from the source with higher provenance priority is returned.<br>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 |
|---|---|
| **Secure LDAP** | Indicates whether the LDAP Server connection is secure or not. |
| **Windows Authentication** | Specifies whether to use Windows Authentication or not.<br>The options are:<br>• None<br>• Negotiate<br>If you select the Negotiate option, the system displays the **Configuration for Windows Authentication** section. |
| **Address** | Specifies the IP address of LDAP Server.<br>This field is mandatory. |
| **Port** | Specifies the port of LDAP Server.<br>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<br>The format of the Bind DN depends on the configuration of the LDAP server.<br>This field is mandatory.<br>**Note:**<br>Even though the parameter name is Bind DN, the format of its value is not limited to the DN format. The format can be any format that the LDAP server can support for LDAP bind. |

| Name | Description |
|---|---|
| | For example: for Active Directory, you can use "domain\user", "user@domain", as well as the actual DN of the user object.<br>For example: for Active Directory, you can use "domain\user", "user@domain", as well as the actual DN of the user object. |
| **Bind Credential** | Specifies the password of the admin user. |
| **Base Context DN** | Specifies the complete Distinguished Name (DN) with the Organizational Unit (OU) for starting the search for users on the enterprise directory.<br>For example: dc=domain,dc=company,dc=com |
| **UID Attribute ID** | Specifies the unique attribute of the user on LDAP.<br>This parameter is used for searching users in the LDAP server.<br>For example: mail<br>This field is mandatory. |
| **Role Filter** | Specifies the search filter that is used to search the roles of the user.<br>For example: (&(objectClass=group) (member={1}) |
| **Role Attribute ID** | Specifies that the user is a member of the groups defined by that attribute.<br>For example: objectCategory<br>This field is mandatory. |
| **Roles Context DN** | Specifies the complete Distinguished Name (DN) to search for a user role, that is, for Role Filter.<br>For example: dc=domain,dc=company,dc=com |
| **Role Name Attribute** | Specifies the name of the role attribute.<br>This field is mandatory only if the **Role Name Attribute Is DN** field is set to true.<br>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.<br>The default value is true. |
| **Allow Empty Passwords** | Indicates whether LDAP Server acknowledges the empty password .<br>The default value is false. |
| **Search Scope** | Specifies the level of the search in the LDAP hierarchy. |

| Name | Description |
|---|---|
| | The options are:<br>• 0: For searching only for the object<br>• 1: For including one level in the LDAP hierarchy in the search<br>• 2: For including subtree in the LDAP hierarchy in the search<br>The default value is 2. |
| **Role Recursion** | Specifies whether role recursion is enabled. The options are:<br>• true<br>• false |
| **Administrator Role** | Specifies the admin role in which the admin users are assigned. |
| **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. |
| **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)<br>• German (de)<br>• English (en)<br>• Spanish (es)<br>• French (fr)<br>• Italian (it)<br>• Japanese (ja)<br>• Korean (ko)<br>• Russian (ru)<br>• Portuguese (pt) |
| **Active Users Search Filter** | Specifies whether the user is active or inactive on LDAP Server. |
| **Last Updated Time Attribute ID** | Specifies when the user is updated on LDAP.<br>For example: whenChanged |

### Configuration for Windows Authentication

| Name | Description |
|---|---|
| **Service Principal Name (SPN)** | Specifies the service principal name<br>UIDAttributeID must be userPrincipalName. |
| **Import keytab file** | Imports the `tomcat.keytab` 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 LDAP Server. |

# Importing an LDAP trusted certificate

## About this task

To use a secure LDAP Server, you must import a trusted certificate.

## Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   The system displays the Enterprise LDAP Server Configuration page.
3. In the **Server Address and Credentials** section, do the following:
   a. Select the **Secure LDAP** check box.
   b. Click **Import Certificate**.
   c. In the Import Certificate window, click **Choose File** and select the certificate from your local system.
   d. Click **Apply**.

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

# Administering the LDAP Server configuration

### Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   The system displays the Enterprise LDAP Server Configuration page.
3. Modify the details of the enterprise directory.
4. Click **Save**.

### Related links

Enterprise LDAP Server Configuration field descriptions on page 16

# Modifying enterprise directory attribute mappings

### Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   The system displays the Enterprise LDAP Server Configuration page.
3. In the Server Address and Credentials section, click **Modify Attribute Mappings**.

   The system displays the Enterprise Directory Mappings page.
4. In the Modify LDAP Attribute Mappings section, modify the value of the attributes.
5. Click **Save**.

# Configuring Windows Authentication for Active Directory

### Before you begin

**Important:**

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

### Procedure

1. Log on to the Avaya Aura® Device Services interface.

2. In the left navigation pane, click **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   The system displays the Enterprise LDAP Server Configuration page.

3. 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. In **UID Attribute ID**, type the sAMAccountName.

      For example, type `mail`.

   d. Ensure that the other settings on the Server Address and Credentials page are appropriate for the LDAP configuration of your Domain Controller.

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

   **Tip:**

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

   a. In **Service Principal Name**, type `HTTP` or `REST_FQDN`.

      For example, type `HTTP` or `aads.example.com`.

   b. To import the `tomcat.keytab` file transferred from the Windows Domain Controller, in **Import keytab file**, click **Import**.

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

      You can use the following command to generate a `tomcat.keytab` file.

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

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

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

   c. In **Kerberos Realm**, type the Kerberos realm, which is usually in uppercase letters.

      For example, `EXAMPLE.COM`.

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

      For example, `example.com`.

   e. In **KDC FQDN**, type the FQDN of the Domain Controller.

      This value also includes the DNS domain at the end.

      For example, `ad.example.com`.

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

g. In a cluster deployment, click **Send Keytab File** to send the `tomcat.keytab` file to a specific node.

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

5. Save the settings to restart the server.

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

# Modifying the provenance priority

### Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   The system displays the Enterprise LDAP Server Configuration page.
3. Click the **Enterprise Directory** tab that you want to use to modify the provenance priority.
4. In the **Provenance Priority** field, click **Modify**.

   The system displays the Source Priority Configuration pop-up window.
5. In the **Provenance Priority** column, type the priority level.

   You can assign a value between 2 to 10. You cannot assign Provenance priority 1as 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.
6. Click **Save**.

# Setting up user synchronization with LDAP Server

### Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Server Connections** > **LDAP Configuration** > **Enterprise Directory**.

   The system displays the Enterprise LDAP Server Configuration page.
3. In the User Synchronization Update Instructions section, do the following:

   a. Specify a date and time to schedule the synchronization of Avaya Aura® Device Services users with the Enterprise LDAP Server users.

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

c. Click **Save**.

4. **(Optional)** To immediately synchronize the user data:

a. Click **Force LDAP Sync**.

b. Click **Save**.

# Adding a trusted host

### Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Server Connections** > **Trusted Hosts**.

   The system displays the Trusted Hosts page.
3. Click **Add**.

   The system displays a new row to add the host.
4. In the new row, type the IP address or FQDN of the trusted host.
5. Click **Save**.

   The system displays the message: `Trusted Hosts data is successfully edited.`

# 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 interface or the Avaya Aura® Device Services configuration script: **`sudo /opt/Avaya/DeviceServices/<aads_version>/CAS/<aads_version>/bin/configureAADS.sh`**.

You can enable CORS for the service and admin interfaces.

### Service Interface

The Service Interface page displays the CORS configuration for the Avaya Aura® Device Services server using the service port 8443.

### Admin Interface

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

## Enabling Cross-Origin Resource Sharing for Service Interface

### Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Server Connections** > **CORS Configuration** > **Service Interface**.

   The system displays the Cross-Origin Resource Sharing for Service interface page.
3. Select the **Enable Cross-Origin Resource Sharing** check box.

   The system displays the **Allow access from any origin** and **Specific Domain(s)** fields.
4. 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.
5. Click **Save**.

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

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

## Enabling Cross-Origin Resource Sharing for Admin Interface

### Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Server Connections** > **CORS Configuration** > **Admin Interface**.

   The system displays the Cross-Origin Resource Sharing for Admin interface page.
3. Select the **Enable Cross-Origin Resource Sharing** check box.

   The system displays the **Allow access from any origin** and **Specific Domain(s)** fields.

4. 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.
5. Click **Save**.

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

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

# Chapter 5: Administering Dynamic Configuration

## Dynamic Configuration service overview

With the Dynamic Configuration service, the system can dynamically retrieve and deploy the device configuration settings to the Avaya Equinox™ clients.

Dynamic Configuration provides a centralized place to administer the user, group, platform, global, exceptions settings. You can configure the Device Configuration settings on the Avaya Equinox™ clients by using one of the following methods:

- DNS-based auto discovery.
- Web address: On the Avaya Equinox™ clients, type the Auto Configuration or Device Configuration URL.

  Example `https://<IP address>:8443/acs/resources/configurations`

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

**Note:**

Authentication domain is an enterprise directory with provenance priority 1. If a user belongs to an authentication domain and a group that is not in the authentication domain, the Dynamic Configuration service still works correctly.

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

- **User:** The User specific settings can be overridden by Platform, Exception, and SMGR settings.
- **Group:** The Group specific settings can be overridden by User, Platform, Exception, and SMGR settings. The LDAP groups are ordered alphabetically.

  If a user belongs to more than one group on LDAP Server, the settings are applied on the basis of the alphabetical order of the group.

**Note:**

The Dynamic Configuration service uses the `memberof` attribute to find the group of the user. By default, the Microsoft Active directory uses these settings. To find the group of the user for the:

- LDS_2012, LDS_2008, OpenLDAP, and OracleDirectoryServer directories, enable the `memberof` attribute.
- Novell directory, use the `groupMembership` attribute.
- Domino directory, use the `dominoAccessGroups` attribute.

For information about these attributes, see the product documentation of these directories. For enabling `memberof` attribute for OpenLDAP, see *OpenLDAP Software 2.4 Administrator's Guide* at http://www.openldap.org/.

- **Platform:** The Platform settings can be overridden by Exception and SMGR settings.
- **Global:** The Global settings can be overridden by any other settings category.
- **Exceptions:** The Exceptions settings are specific to SMGR Home Location.

### Home Location settings

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

On the System Manager Web Console, you can configure:

- Dial-plan rules on the **Routing** > **Dial Patterns** page.
- Home location of a user on the **Routing** > **Locations** page.

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

### ESMSRVR setting

The ESMSRVR setting is retrieved from the **IM Gateway SIP Entity** field from Presence Profile on System Manager. Therefore, if Presence Profile is assigned to a user on System Manager, then the system overrides the value from Presence Profile to any locally configured ESMSRVR value at Group and Global levels. So the system uses the Presence Profile value for configuration.

## Viewing Home Location

### Procedure

1. On the home page of the System Manager Web Console, click **User Management** > **Manage Users**.
2. Select a user and click **View**.
3. In the **Communication Profile** tab, click the arrow next to the **Session Manager Profile** section.

The system displays the **Home Location** in the Call Routing Settings section.

## Implementation of the Dynamic Configuration settings

In Dynamic Configuration, different settings that are common at User, Group, Platform, Global, and Exceptions levels have different priorities. The administrator must take this into account while creating Dynamic Configurations.

The Dynamic Configuration service collects settings from the following levels:

- ACCOUNT/SMGR SETTINGS
- EXCEPTION SETTINGS
- PLATFORM
- USER
- GROUP
- GLOBAL
- CUSTOM FILE SETTINGS

If the same settings from different levels are applied to a user, the system overrides the settings in the following order: SMGR > Exceptions > Platform > User > Group > Global > Custom. For example, if a setting is specified at both the Platform and Group levels, the system overrides the value with the Platform level settings.

### Example

If administrators have users in two LDAP groups, the users in Group 1 use Avaya Multimedia Messaging, but users in Group 2 cannot use Avaya Multimedia Messaging. To configure this, the administrator must set the ESMENABLED setting for each group. This setting is available at the USER, GROUP, PLATFORM, and GLOBAL levels.

### Solution

This setting is specific to the LDAP group, so the ESMENABLED setting must be configured on the GROUP level. The configuration for users is as follows:

- In Group 1 must be set to ESMENABLED =1
- In Group 2 must be set to ESMENABLED =0

After creating the configuration, publish the settings for users in Group 1 and Group 2.

**Note:**

In this case, do not configure the ESMENABLED setting at the PLATFORM level.

# Creating a new configuration

## About this task

You can create a new configuration that can be applied to the following: a user, a group, a platform, and all users. A new configuration can also be applied to exceptions, such as settings specific to System Manager.

## Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Dynamic Configuration** > **Configuration**.

   The system displays the Configuration page.
3. In the User, Group, Platform, Global, or 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 templates.
4. Click **Save**.
5. In the Save Configuration window, select **Create new configuration** and type a name for the specified configuration.
6. Click **Save**.

   The system displays a message that the configuration is saved successfully.

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

## Related links

Configuration settings on page 31
Configuration field descriptions on page 30

# 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. |
| **Group** | Displays the **Group**, **Platform**, and **Global** settings for the selected group. |
| **Platform** | Specifies a platform to retrieve the data.<br>• iOS<br>• Android |

| Name | Description |
|---|---|
| | • Windows<br>• Mac |
| **USER**, **Group**, **Platform**, **Global**, 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. |
| **Settings configured on SMGR** | The system displays this section for the users.<br>Displays the read-only settings. To edit the values, go to the SMGR configuration. |
| **Category** | Specifies the category for the group settings. |

| Button | Description |
|---|---|
| **Retrieve** | Retrieves the settings based on the search criteria. |
| **Save** | Saves a new test configuration.<br>Overwrites an existing configuration. |
| **Test** | Provides a test URL to test the configuration settings. |
| **Publish** | Publishes the configuration settings. |
| **Delete** | Deletes the selected configuration. |

## 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, take the mouse over the icon that is beside the setting name.

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

- CONFIG_SERVER
- CONFIG_SERVER_SECURE_MODE
- ENABLE_PRESENCE

## System parameters

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| MODEL | A string of maximum 10 characters that identifies the endpoint platform and version. This value is built into the application as an identifier for the endpoint or release to allow it to be used in conditional statements. The platform names are abbreviated.<br>For Release 3.0:<br>• aca.3.0 is the value for Avaya Equinox™ for Android.<br>• aci.3.0 is the value for Avaya Equinox™ for iOS.<br>• acm.3.0 is the value for Avaya Equinox™ for Mac.<br>• acw.3.0 is the value for Avaya Equinox™ for Windows. | Supported on all platforms. |
| MODEL4 | A string of maximum 4 characters that identifies the endpoint platform. This value is built into the application as an identifier for the endpoint or release to allow it to be used in conditional statements.<br>For example, acm is the value for Avaya Equinox™ for Mac. | Supported on all platforms. |

## SIP parameters

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| SIPENABLED | The parameter that indicates whether the SIP service is enabled.<br>The options are:<br>• 1: Indicates enabled.<br>• 0: Indicates disabled. This is the default value. | Supported on all platforms. |
| SIP_CONTROLLER_LIST | A list of SIP controller designators, separated by commas without any intervening spaces, where each controller designator has the | Supported on all platforms. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| | following format: `host[:port][;transport=xxx]`<br>Example: `proxy1:5061;transport=tls,proxy2:5061;transport=tls`.<br>**Note:**<br>• The parameter value can be an FQDN or an IP address.<br>• If you use this parameter in combination with LOCKED_PREFERENCES and OBSCURE_PREFERENCES, all three associated UI fields are locked. The SIP fields are Server Address, Server Port, and Use TLS. | |
| SIPDOMAIN | The SIP domain. | Supported on all platforms. |
| SIPSSO | The parameter that indicates whether unified login is enabled.<br>The options are:<br>• 1: Indicates enabled.<br>• 0: Indicates disabled. This is the default value. | Supported on all platforms. |
| SIPUSERNAME | The SIP account name. | Supported on all platforms. |
| SIPPASSWORD | The SIP account password. | Supported on all platforms. |
| ENABLE_MDA_JOIN | The parameter to enable MDA Join if you are using a version of Communication Manager later than 6.3.<br>The options are:<br>• 1: Indicates enabled.<br>• 0: Indicates disabled. This is the default value.<br>On Communication Manager 6.3 and earlier versions, there is an issue that causes Communication Manager to reset if a user attempts to bridge into an active call from their MDA extension. Hence, by default, the remote line appearance Join button is disabled. | Supported on all platforms. |
| COMM_ADDR_HANDLE_TYPE | A virtual configuration setting that defines SIP handle subtype for the user.<br>The SIP handle subtype setting is used to select correct SIP handle for the Avaya Aura® | Supported only on Avaya Aura® Device Services. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| | System Managerusers. The system does not send virtual settings to endpoints and these settings are for the Dynamic Configuration service internal usage only.<br>AutoConfig Service does not respond with SIPUSERNAME and SIPDOMAIN if COMM_ADDR_HANDLE_TYPE is not configured.<br>The options are:<br>• Avaya SIP: Only numeric SIP handles of subtype Avaya SIP will be retrieved from System Manager. The system ignores all the other alphanumeric SIP handles of Avaya SIP subtype.<br>• Avaya E.164: A maximum of fifteen digits and a plus (+) prefix will be retrieved from System Manager.<br>• 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.<br>This field is mandatory if you select Avaya SIP for COMM_ADDR_HANDLE_TYPE.<br>Accepted values are 1 to 255. | Supported only on Avaya Aura® Device Services. |

## Unified login parameters

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| SSOENABLED | The parameter that indicates whether unified login is enabled.<br>The options are:<br>• 1: Indicates enabled. This is the default value.<br>• 0: Indicates disabled. | Supported on all platforms. |
| SSOUSERID | The unified login user ID. | Supported on all platforms. |
| SSOPASSWORD | The unified login password. | Supported on all platforms. |

## Automatic configuration parameters

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| AUTOCONFIG_USESSO | The parameter that indicates whether the endpoint uses the unified login credentials during the retrieval of the `46xxsettings` file. Else, the assumption is that automatic configuration credentials are unique.<br>The options are:<br>• 1: Indicates that the automatic configuration credentials are the same as the unified login credentials. This is the default value.<br>• 0: Indicates that the automatic configuration credentials are unique. | Supported on all platforms. |
| SETTINGS_CHECK_INTERVAL | The interval used to define how often endpoints will check for settings file changes.<br>The range for this parameter is 0 to 30 days. The default is 0 that indicates never. | Supported on all platforms. |
| SETTINGS_FILE_URL | The URL to move settings files from one server to another. This URL is used during the next check interval if defined. | Supported on all platforms. |

## Conferencing parameters

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| CONFERENCE_FACTORY_URI | The URL that defines the adhoc conference resource to be used by the endpoint.<br>This is an optional parameter. Hence, the value can be null. | Supported on all platforms. |
| CONFERENCE_ACCESS_NUMBER | The default conference access number. | Supported on all platforms. |
| CONFERENCE_PORTAL_URI | The URI of the conference portal.<br>This parameter enables the client UI to launch the conference portal. | Supported on all platforms. |
| CONFERENCE_MODERATOR_CODE | The conference moderator code. | Supported on all platforms. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| | Users can click to join their own bridge through a UC client. | |
| CONFERENCE_PARTICIPANT_CODE | The conference participation code.<br>Users can share their participant code with other users in Calendar invites and through the Share My Bridge feature. | Supported on all platforms. |
| CONFERENCE_VIRTUAL_ROOM | The Scopia Virtual Room ID for the virtual room owner. | Supported on all platforms. |
| CONFERENCE_FQDN_SIP_DIAL_LIST | A list of Scopia conference bridges that can support SIP Enhanced Conference Experience. | Supported on all platforms. |
| UCCPENABLED | The parameter to enable or disable UCCP Conferencing protocol in the client.<br>The options are:<br>• 1: Indicates that the UCCP Conferencing protocol is enabled in the client. This is the default value.<br>• 0: Indicates that the UCCP Conferencing protocol is disabled in the client. SIP CCMP is used for conferencing.<br>**Note:**<br>If you do not include this parameter in the auto-configuration file or manually configure the settings in the Avaya Equinox™ client, this parameter is enabled by default for desktop clients. | Supported on all platforms. |

## Automatic software updates parameters

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| APPCAST_ENABLED | The parameter that indicates whether the service is enabled.<br>The options are:<br>• 1: Indicates enabled.<br>• 0: Indicates disabled. This is the default value. | Supported on Avaya Equinox™ for Mac and Windows. |
| APPCAST_URL | The URL that defines the appcast feed used by the endpoints. | Supported on Avaya Equinox™ for Mac and Windows. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| APPCAST_CHECK_INTERVAL | The interval at which endpoints check for software updates.<br>The range for this parameter is 0 to 30 days. The default is 0 that indicates never. | Supported on Avaya Equinox™ for Mac and Windows. |

## Avaya Multimedia Messaging parameters

Use the following automatic configuration parameters if you have configured the Avaya Equinox™ clients to interwork with Avaya Multimedia Messaging.

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| ESMENABLED | The parameter that indicates whether Avaya Multimedia Messaging is enabled.<br>The options are:<br>• 1: Indicates enabled.<br>• 0: Indicates disabled. This is the default value. | Supported on all platforms. |
| ESMSSO | The parameter that indicates whether the Avaya Multimedia Messaging service uses unified login.<br>The options are:<br>• 1: Indicates that Avaya Multimedia Messaging uses unified login. This is the default value.<br>• 0: Indicates that Avaya Multimedia Messaging does not use unified login. | Supported on all platforms. |
| ESMUSERNAME | The Avaya Multimedia Messaging account user name. | Supported on all platforms. |
| ESMPASSWORD | The Avaya Multimedia Messaging account password. | Supported on all platforms. |
| ESMSRVR | The IP address or fully qualified domain name of the Avaya Multimedia Messaging server. | Supported on all platforms. |
| ESMPORT | The port of the Avaya Multimedia Messaging server.<br>The default value is 8443. | Supported on all platforms. |
| ESMSECURE | The parameter that indicates whether TLS is being used. | Supported on all platforms. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| | The options are:<br>• 1: Indicates that TLS is used. This is the default value.<br>• 0: Indicates that TLS is not used. | |
| ESMREFRESH | The parameter that indicates the Avaya Multimedia Messaging refresh interval in minutes.<br>The valid values are 0, 10, 30, and 60.<br>The default value is 0, which indicates continuous mode.<br>**Note:**<br>The manual mode option is no longer supported. | Supported on all platforms. |
| ESMHIDEONDISCONNECT | The parameter to hide Avaya Multimedia Messaging conversations and message details in the Messages screen and Messaging area of the Top Of Mind screen when not connected to Avaya Multimedia Messaging.<br>The options are:<br>• 1: Indicates enabled.<br>• 0: Indicates disabled. This is the default value. | Supported on Avaya Equinox™ for Android and iOS. |

## Avaya Aura® Device Services parameters

Use the following automatic configuration parameters if you have configured the Avaya Equinox™ clients to interwork with Avaya Aura® Device Services.

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| ACSENABLED | The parameter that indicates whether Avaya Aura® Device Services is enabled.<br>The options are:<br>• 1: Indicates enabled.<br>• 0: Indicates disabled. This is the default value. | Supported on all platforms. |
| ACSSRVR | The Avaya Aura® Device Services IP address or FQDN. | Supported on all platforms. |
| ACSPORT | The Avaya Aura® Device Services port. | Supported on all platforms. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| | The default value is 443. | |
| ACSSECURE | The parameter that indicates whether TLS is being used.<br>The options are:<br>• 1: Indicates that TLS is used. This is the default value.<br>• 0: Indicates that TLS is not used. | Supported on all platforms. |
| ACSSSO | The parameter that indicates whether Avaya Aura® Device Services uses unified login.<br>The options are:<br>• 1: Indicates that Avaya Aura® Device Services uses unified login. This is the default value.<br>• 0: Indicates that Avaya Aura® Device Services does not use unified login. | Supported on all platforms. |
| ACSUSERNAME | The Avaya Aura® Device Services user name. | Supported on all platforms. |
| ACSPASSWORD | The Avaya Aura® Device Services password. | Supported on all platforms. |

## Client Enablement Services parameters

Use the following parameters if Avaya Equinox™ for Android and iOS are configured to interwork with Client Enablement Services. Client Enablement Services is not supported on Avaya Equinox™ for Mac and Windows.

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| CESENABLED | The parameter that indicates whether Client Enablement Services is enabled.<br>The options are:<br>• 1: Indicates enabled.<br>• 0: Indicates disabled. This is the default value. | Supported on Avaya Equinox™ for Android and iOS. |
| CESSSO | The parameter that indicates whether Client Enablement Services uses unified login.<br>The options are:<br>• 1: Indicates that Client Enablement Services uses unified login. This is the default value. | Supported on Avaya Equinox™ for Android and iOS. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| | • 0: Indicates that Client Enablement Services does not use unified login. | |
| CESUSERNAME | The Client Enablement Services account name. | Supported on Avaya Equinox™ for Android and iOS. |
| CESPASSWORD | The Client Enablement Services account password. | Supported on Avaya Equinox™ for Android and iOS. |
| CESSRVR | The IP address or fully qualified domain name of the Client Enablement Services server. | Supported on Avaya Equinox™ for Android and iOS. |
| CESPORT | The Client Enablement Services server port.<br>The default value is 7777. | Supported on Avaya Equinox™ for Android and iOS. |
| CESSECURE | The parameter that indicates whether TLS is being used.<br>The options are:<br>• 1: Indicates that TLS is used. This is the default value.<br>• 0: Indicates that TLS is not used.<br>**Note:**<br>Avaya Equinox™ 3.0 only supports TLS connections to Client Enablement Services. The user cannot change this value from the Settings menu in the application. | Supported on Avaya Equinox™ for Android and iOS. |
| CESVMPIN | The voice mail PIN required for visual voice mail. | Supported on Avaya Equinox™ for Android and iOS. |

## Desktop parameter

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| DESKTOP_HTTP_APPLICATION_INTEGRATION | The parameter to disable Desktop HTTP Application Integration.<br>This parameter controls whether the client API is on or off, which in turn controls experiences such as the headset API and the browser plug-ins. The options are:<br>• 1: Indicates that Desktop HTTP Application Integration is | Supported on Avaya Equinox™ for Mac and Windows. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| | enabled. This is the default value.<br>• 0: Indicates that Desktop HTTP Application Integration is disabled. | |

## EC500 parameters

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| EC500ENABLED | The parameter that indicates whether EC500 is enabled.<br>The options are:<br>• 1: Indicates enabled.<br>• 0: Indicates disabled. This is the default value. | Supported on Avaya Equinox™ for Android and iOS. |
| EC500VOICEMAILNUMBER | The voice mail system access number.<br>Endpoints can retrieve this value from multiple sources. A summary of this logic is:<br>• With SIP, the number comes from the PPM protocol, which pulls the configuration from Avaya Aura®.<br>• With Client Enablement Services, the number comes from the Client Enablement Services server.<br>• In other situations, the number comes from this parameter. | Supported on Avaya Equinox™ for Android and iOS. |
| FNUIDLEAPPEARANCESELECT | The number to dial for the Idle Appearance Select feature.<br>This number is used to identify an idle line on your extension when you make a call. | Supported on Avaya Equinox™ for Android and iOS. |
| FNUSIMRINGENABLE or FNUOFFPBXCALLENABLE | The number to dial for enabling Off-PBX calls.<br>This number is used to enable your mobile phone to ring when you receive a call on your deskphone. | Supported on Avaya Equinox™ for Android and iOS. |
| FNUSIMRINGDISABLE or FNUOFFPBXCALLDISABLE | The number to dial for disabling Off-PBX calls.<br>This number is used to disable your mobile phone from ringing when you receive a call on your deskphone. | Supported on Avaya Equinox™ for Android and iOS. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| FNUCFWDENABLE or FNUCFWDALL | The number to dial for enabling call forwarding for all calls. | Supported on Avaya Equinox™ for Android and iOS. |
| FNUCFWDDISABLE or FNUCFWDCANCEL | The number to dial for canceling call forwarding. | Supported on Avaya Equinox™ for Android and iOS. |
| FNUACTIVEAPPEARANCESELECT | The number to dial for the Active Appearance Select feature.<br>This number is used to join an active call on your deskphone using your mobile phone. | Supported on Avaya Equinox™ for Android and iOS. |
| FNUSACENABLE | The number to dial for enabling the Send All Calls feature.<br>This number is used to send all calls to a predefined number set on the server by the administrator. | Supported on Avaya Equinox™ for Android and iOS. |
| FNUSACCANCEL | The number to dial for disabling the Send All Calls feature.<br>This number is used to disable the sending of all calls to a predefined number set on the server by the administrator. | Supported on Avaya Equinox™ for Android and iOS. |
| FNE_SETUP_DELAY | The parameter that indicates the delay in seconds between the EC500 call being placed and the transmission of the digits for EC500.<br>The default value is 3 seconds.<br>The purpose of this setting is to address call setup delays with specific regions and trunk providers. | Supported on Avaya Equinox™ for Android and iOS. |
| STATION_SECURITY_ENABLED | The parameter that indicates whether EC500 station security is enabled. The station security code reduces the risk of toll fraud.<br>The options are:<br>• 1: Indicates that EC500 station security is enabled.<br>• 0: Indicates that EC500 station security is disabled. This is the default value. | Supported on Avaya Equinox™ for Android and iOS. |

## Dialing rule parameters

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| ENHDIALSTAT | The parameter that indicates whether dialing rules are enabled. | Supported on all platforms. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| | The options are:<br>• 1: Indicates enabled.<br>• 0: Indicates disabled. This is the default value. | |
| PHNOL | The number to dial to access an external line. | Supported on all platforms. |
| PHNCC | The country code. | Supported on all platforms. |
| SP_AC or DIALPLANAREACODE | The area or city code. | Supported on all platforms. |
| PHNPBXMAINPREFIX or DIALPLANPBXPREFIX | The PBX main prefix. | Supported on all platforms. |
| PHNLD | The number to dial for long distance calls. | Supported on all platforms. |
| PHNIC | The number to dial for international calls. | Supported on all platforms. |
| PHNDPLENGTH | The internal extension length. | Supported on all platforms. |
| DIALPLANEXTENSIONLENGTHLIST | A list of PHNDPLENGTH values separated by commas.<br>This parameter takes precedence over PHNDPLENGTH. | Supported on all platforms. |
| PHNLDLENGTH | The length of national phone numbers. | Supported on all platforms. |
| DIALPLANNATIONALPHONENUMLENGTHLIST | A list of PHNLDLENGTH values separated by commas.<br>This parameter takes precedence over PHNLDLENGTH. | Supported on all platforms. |
| PHNREMOVEAREACODE or DIALPLANLOCALCALLPREFIX | The parameter that indicates whether the area code must be removed for local calls.<br>The options are:<br>• 1: Indicates enabled. Area code is removed for local calls.<br>• 0: Indicates disabled. Area code is not removed for local calls. This is the default value. | Supported on all platforms. |
| AUTOAPPLY_ARS_TO_SHORTNUMBERS | The parameter to disable the dialing rule logic that automatically appends the ARS code to numbers that are shorter than the shortest extension length. | Supported on all platforms. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| | The options are:<br>• 1: Indicates enabled. This is the default value.<br>• 0: Indicates disabled. | |
| APPLY_DIALINGRULES_TO_PLUS_NUMBERS | The parameter to replace the plus sign (+) with dial plan digits.<br>When possible, configure the plus (+) dialing option in Session Manager instead of enabling this parameter.<br>The options are:<br>• 1: Indicates true.<br>• 0: Indicates false. This is the default value. | Supported on all platforms. |

## Presence parameters

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| PRESENCE_SERVER | The Presence Services server address. | Supported on Avaya Equinox™ for Windows. |
| DND_SAC_LINK | The parameter that activates the Send All Calls feature when the user sets the presence status to Do Not Disturb.<br>The options are:<br>• 1: Indicates that the Send All Calls feature is activated.<br>• 0: Indicates that the Send All Calls feature is not activated. This is the default value. | Supported on all platforms. |
| WINDOWS_IMPROVIDER | The parameter that indicates whether a UC client is the IM provider for Windows clients.<br>The options are:<br>• 1: Indicates that a UC client is the IM provider for Windows clients. This is the default value.<br>• 0: Indicates that a UC client is not the IM provider for Windows clients. | Supported on Avaya Equinox™ for Windows. |

## LDAP parameters

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| DIRENABLED | The parameter that indicates whether LDAP is enabled.<br>The options are:<br>• 1: Indicates enabled.<br>• 0: Indicates disabled. This is the default value. | Supported on Avaya Equinox™ for Mac and Windows. |
| DIRSSO | The parameter that indicates whether to use unified login.<br>The options are:<br>• 1: Indicates Yes. This is the default value.<br>• 0: Indicates No. | Supported on Avaya Equinox™ for Mac and Windows. |
| DIRSRVR | The IP address or fully qualified domain name of the LDAP server. | Supported on Avaya Equinox™ for Mac and Windows. |
| DIRSRVRPRT | The port number for the LDAP server.<br>The default value is 636. | Supported on Avaya Equinox™ for Mac and Windows. |
| DIRUSERNAME | The LDAP authentication user name. | Supported on Avaya Equinox™ for Mac and Windows. |
| DIRPASSWORD | The LDAP authentication password. | Supported on Avaya Equinox™ for Mac and Windows. |
| DIRTOPDN | The LDAP search base. | Supported on Avaya Equinox™ for Mac and Windows. |
| DIRSECURE | The parameter that indicates whether to use TLS or TCP for LDAP.<br>The options are:<br>• 1: Indicates TLS. This is the default value.<br>• 0: Indicates TCP. | Supported on Avaya Equinox™ for Mac and Windows. |
| DIRIMATTRIBUTE | The client provides access to the enterprise directory search using a direct LDAP connection. While processing the results, the client can process the attribute, such as telephoneNumber, specified in this parameter as an instant messaging address.<br>For example, telephoneNumber, as often the administrator provisions users with Presence Server instant messaging addresses that correspond to the telephone number of the user. | Supported on Avaya Equinox™ for Mac and Windows. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| | The default value is mail. | |
| DIRUSEIMDOMAIN | The parameter that indicates whether the client must perform a mapping to the IM domain.<br>The options are:<br>• 1: Indicates enabled. This is the default value.<br>• 0: Indicates disabled.<br>In this parameter, the telephone number of the user is mapped into the IM domain.<br>Example: 16135551212 becomes `16135551212@presence.example.com` if the IM domain is presence.example.com.<br>This parameter is also used if an email address field is used. For example, alice@example.com becomes `alice@presence.example.com`.<br>This parameter is only enabled in single domain deployments. You must not use domain mapping if any form of messaging federation is in place. Instead, ensure that the correct IM address is stored in an LDAP attribute. | Supported on Avaya Equinox™ for Mac and Windows. |
| DIRTYPE | The type of LDAP directory to which the endpoint connects.<br>Valid values are:<br>• ACTIVEDIRECTORY: This is the default value.<br>• DOMINO<br>• NOVELL | Supported on Avaya Equinox™ for Mac and Windows. |
| DIRSCOPE | The parameter that defines the scope of the LDAP search.<br>Valid values are:<br>• LDAP_SCOPE_BASE<br>• LDAP_SCOPE_ONELEVEL<br>• LDAP_SCOPE_SUBTREE: This is the default value. | Supported on Avaya Equinox™ for Mac and Windows. |
| DIRTIMEOUT | The search time-out interval in seconds. | Supported on Avaya Equinox™ for Mac and Windows. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| | The range is 10 to 200 and the default value is 100. | |
| DIRMAXENTRIES | The maximum number of matching entries to display.<br>The range is 10 to 100 and the default value is 50. | Supported on Avaya Equinox™ for Mac and Windows. |

## Media parameters

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| DTMF_PAYLOAD_TYPE | The RTP payload type to be used for RFC 2833 signaling.<br>Valid values are 96 through 127.<br>The default value is 120. | Supported on all platforms. |
| RTP_PORT_LOW | The lower limit of the UDP port range to be used by RTP/RTCP or SRTP/SRTCP connections.<br>Valid values are 1024 through 65503.<br>The default value is 5004. | Supported on all platforms. |
| RTP_PORT_RANGE | The range or number of UDP ports available for RTP/RTCP or SRTP/SRTCP connections.<br>This value is added to RTP_PORT_LOW to determine the upper limit of the UDP port range.<br>Valid values are 32 through 64511.<br>The default value is 40. | Supported on all platforms. |
| ECHO_CANCELLATION | The echo cancellation algorithm. Echo cancellation is a process that removes echo from a voice communication to improve voice quality on a telephone call.<br>The supported values are:<br>• aec: This is the default value.<br>• aecm<br>• off | Supported on Avaya Equinox™ for Android. |
| MEDIAENCRYPTION | The parameter to specify the media encryption ciphers. The default value is 10,11,1,2,9, where:<br>• 1: Indicates aescm128-hmac80 | Supported on all platforms. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| | • 2: Indicates aescm128-hmac32<br>• 9: Indicates none<br>• 10: Indicates aescm256-hmac80<br>• 11: Indicates aescm256-hmac32<br>Avaya Equinox™ supports any combinations of 1, 2, 10, 11, and 9, such as 1,9 or 2,9 or 1,2,9 or 10,9 or 11,9 or 10,11,9 or 1,2,10,11,9. The ordering of these digits is ignored by Avaya Equinox™ and does not affect the functionality.<br>To support the Best Effort SRTP negotiation, the parameter must contain 9 and at least one other value of 1,2,10,11. If the parameter does not contain 9, Avaya Equinox™ automatically adds 9.<br>For interoperability with Avaya Aura®:<br>• For the Avaya Aura® 6.x environment, the recommended value for this parameter is 1,9.<br>• For the Avaya Aura® 7.x environment, the recommended value for this parameter is 10,1,9. | |
| ENCRYPT_SRTCP | The default value is 0. | Supported on all platforms. |

## Video parameters

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| ENABLE_VIDEO | The parameter that indicates whether video is enabled.<br>The options are:<br>• 1: Indicates enabled. This is the default value.<br>• 0: Indicates disabled. | Supported on all platforms. |
| VIDEO_MAX_BANDWIDTH_ANY_NETWORK | The parameter that indicates the video bandwidth on any network.<br>The supported values in kilobits per second (kbps) are:<br>• 1792 | Supported on all platforms. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| | • 1280: Default value for Windows clients.<br>• 1024: Default value for MacOS clients.<br>• 768<br>• 512: Default value for mobile clients.<br>• 384<br>• 256<br>• 128<br>• 0. This indicates that video is blocked.<br>You can also specify a custom value between 0 to 10000. | |
| VIDEO_MAX_BANDWIDTH_CELLULAR_DATA | The parameter that indicates the video bandwidth on the cellular data network.<br>The supported values are the same as for VIDEO_MAX_BANDWIDTH_ANY_NETWORK.<br>The default value is 512 kbps to limit the video resolution. | Supported on Avaya Equinox™ for Android and iOS. |
| BFCP_TRANSPORT | The parameter to enable or disable Binary Floor Control Protocol (BFCP) and set the Transport mode.<br>The options are:<br>• 1: Indicates UDP only.<br>• 0: Indicates that BFCP is disabled. This is the default value. | Supported on Avaya Equinox™ for Mac. |
| BFCP_UDP_MINIMUM_PORT | The parameter that specifies the lower limit of the UDP port range to be used by the BFCP signalling channel. The range is 1024 to 65503.<br>The default value is 5204.<br>Usually, the BFCP minimum port value is equal to the RTP UDP port maximum value + 1. | Supported on Avaya Equinox™ for Mac. |
| BFCP_UDP_MAXIMUM_PORT | The parameter that specifies the upper limit of the UDP port range to be used by the BFCP signalling channel. The range is 1024 to 65503.<br>The default value is 5224. | Supported on Avaya Equinox™ for Mac. |

## Voice mail parameter

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| AAM_PORTAL_URI | The URI of Avaya Aura® Messaging Web Portal.<br>This parameter allows users to start the voice mail portal on their client for advanced interactions, such as downloading voice mail or adjusting settings. | Supported on Avaya Equinox™ for Mac and Windows. |

## Administration parameters

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| SUPPORTEMAIL | The default email address to send diagnostic logs. | Supported on all platforms. |
| SUPPORTURL | The default URL to get support. | Supported on all platforms. |
| LOG_VERBOSITY | The parameter that indicates whether verbose logging is enabled in the local client.<br>The options are:<br>• 1: Indicates enabled.<br>• 0: Indicates disabled. This is the default value. | Supported on all platforms. |
| ANALYTICSENABLED | The parameter that allows administrators to stop collecting data on behalf of their user community.<br>The options are:<br>• 1: Indicates enabled. This is the default value.<br>• 0: Indicates disabled. | Supported on all platforms. |
| ISO_SYSTEM_LANGUAGE | The parameter that indicates the system language if silent installation is used.<br>The default language is the same as the language of the operating system if supported. Else, the default language is set to en_US. | Supported on Avaya Equinox™ for Mac and Windows. |
| CELLULAR_DIRECT_ENABLED | The parameter that indicates whether the Cellular Direct feature is enabled.<br>The options are:<br>• 1: Indicates enabled. | Supported on Avaya Equinox™ for Android and iOS. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| | • 0: Indicates disabled. This is the default value. | |
| CELLULAR_DIRECT_NUMBER_LIST | A multivalue parameter that is a number of phone numbers that are sent directly to the native phone client on iOS or Android. The numbers can contain any digits or characters that can be dialed from the client UI or the native dialer, including:<br>• Special characters, such as plus (+), asterisk (*), and hash (#).<br>• Any alphanumeric character, such as A-Z, a-z, or 0-9.<br>**Note:**<br>iOS does not support numbers containing an asterisk (*) or a hash (#). | Supported on Avaya Equinox™ for Android and iOS. |

## Security settings parameter

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| REVOCATIONCHECKENABLED | The parameter that indicates whether certificate revocation is checked. Supported values are:<br>• 0: Disabled.<br>• 1: Best effort.<br>The default value for checking certificate revocation. The revocation checking failures, such as no response and no revocation authority, are not fatal.<br>• 2: Mandatory.<br>Certificate revocation is checked. Revocation checking failures are fatal. | Supported on Avaya Equinox™ for Mac and Windows. |
| TLSSRVRID | The parameter that defines the actions to be taken when the | Supported on all platforms. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| | server identity validation fails. Supported values are:<br>• 0: Allow the connection to continue. This is the default value.<br>• 1: Abort the connection.<br>This parameter applies to all protocols for all configured services on the endpoint.<br>**Note:**<br>If you correct the Subject Alternative Name value in the System Manager certificate after a server identity validation failure, you must inform the user to log in again to Avaya Equinox™. | |
| SUPPORTWINDOWSAUTHENTICATION | The parameter that indicates whether Windows Authentication is used when challenged for authentication on a device that is logged in to the domain.<br>Supported values are:<br>• 1: Enabled. This is the default value.<br>• 0: Disabled. | Supported on Avaya Equinox™ for Windows. |

## User policy settings parameters

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| LOCKED_PREFERENCES | The list of locked preferences.<br>For example, `SET LOCKED_PREFERENCES "CESSRVR","CESPORT","CESENABLED".`<br>The user cannot modify the values of the locked preferences in the client as locked preferences appear as read only.<br>To reset locked preferences, use `SET LOCKED_PREFERENCES ""`.<br>The name for a setting must be the same across all clients. | Supported on all platforms. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| | The default value is Not locked. | |
| OBSCURE_PREFERENCES | The list of obscured preferences.<br>The default value is Not obscured.<br>If you specify any parameters in this attribute, Avaya Equinox™ makes the value read-only. Also, the data itself is hidden from viewing by end-users. | Supported on all platforms. |
| VOIPCALLINGENABLED | The parameter that indicates whether VoIP is used to make calls. The supported values are:<br>• 0: Never.<br>• 1: Always. This is the default value.<br>• 2: Wifi only. | Supported on Avaya Equinox™ for Android and iOS. |
| TRUSTCERTS | The list of URLs, absolute or relative, to CA certificates that will be stored in the private trust store and used to validate certificates of the various servers.<br>Set a blank value to clear the private trust store and go back to the platform trust store.<br>Certificates stored in binary DER form, commonly known as `.cer`, `.crt`, or `.der` files, and Base64-encoded DER form, commonly known as `.pem` files, are supported. | Supported on all platforms. |
| DISABLE_PASSWORD_STORAGE | The parameter that stops the client from storing passwords locally.<br>The options are:<br>• 1: Indicates TRUE.<br>• 0: Indicates FALSE. This is the default value.<br>The client can continue to cache the credentials in RAM only, when enabled. The client does not store passwords in persistent storage. This implies that each time the client starts, users are prompted to enter their password. | Supported on all platforms. |
| FORCE_LOGOUT_AFTER | The parameter that represents the number of days before the client automatically logs out and forces users to enter their credentials to log in again.<br>The range is from 0 to 365 days. | Supported on Avaya Equinox™ for Android and iOS. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| | The options are:<br>• 1: Indicates enabled.<br>• 0: Indicates disabled. This is the default value. | |

## User preferences parameters

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| AUTO_AWAY_TIME | The parameter that indicates the idle time in minutes after which the presence status of the user automatically changes to Away.<br>The value is normalized to 0, 5, 10, 15, 30, 60, 90, or 120. A value of 0 disables the feature.<br>The default value is 10 minutes.<br>**Note:**<br>The value of 5 minutes is only supported on desktop clients. | Supported on all platforms. |
| ADDRESS_VALIDATION | The parameter that indicates whether messaging address validation is enabled.<br>The options are:<br>• 1: Indicates enabled.<br>• 0: Indicates disabled. This is the default value. | Supported on all platforms. |
| PHONE_NUMBER_PRIORITY | The default phone number priority.<br>The value is a list of comma separated strings, which are listed from left to right to indicate the order in which the phone numbers will be used.<br>If the PHONE_NUMBER_PRIORITY parameter is not defined, then the default order is used, which is Work, Mobile, Home. | Supported on all platforms. |
| NAME_SORT_ORDER | The parameter that indicates how names are sorted in the UI.<br>The value is a comma-separated list of the following strings:<br>• last<br>• first | Supported on Avaya Equinox™ for Android and Windows. |

| Name | Description | Avaya Equinox™ platform support |
|---|---|---|
| | By default, names are sorted according to last name. | |
| NAME_DISPLAY_ORDER | The parameter that indicates how names are displayed in the UI.<br>The value is a comma-separated list of the following strings:<br>• last<br>• first<br>By default, the first name is displayed first. | Supported on Avaya Equinox™ for Android and Windows. |
| HOMESCREENLAYOUT | The parameter that defines which Home screen layout to show:<br>• # Default (Top Of Mind): SET HOMESCREENLAYOUT 0. This is the default value.<br>• # Top Of Mind: SET HOMESCREENLAYOUT 1<br>• # Top Of Mind Lite: SET HOMESCREENLAYOUT 2 | Supported on Avaya Equinox™ for Android and iOS. |
| APPLICATION_AUTO_START | The parameter that is used to start the client automatically.<br>The values are:<br>• 1: Yes.<br>• 0: No. This is the default value. | Supported on Avaya Equinox™ for Android, Mac, and Windows. |
| APPLICATION_CLOSE_WINDOW | The parameter that indicates how the client behaves when the user clicks **X**. The supported values are:<br>• 0: Minimize the client to the task bar or dock bar. This is the default value.<br>• 1: Minimize the client to the notification area.<br>• 2: Exit the client. | Supported on Avaya Equinox™ for Mac and Windows. |

# 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, exceptions, and all users.

### Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Dynamic Configuration** > **Configuration**.

   The system displays the Configuration page.
3. In the **User**, **Group**, **Platform**, **Global**, or **Exceptions** sections, specify the settings.
4. Click **Save**.
5. In the Save Configuration window, select **Overwrite existing configuration** and select an existing configuration.
6. Click **Save**.

   The system overwrites the configuration settings to an existing configuration.

## Testing configuration settings

### Before you begin

Get admin credentials.

### Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Dynamic Configuration** > **Configuration**.

   The system displays the Configuration page.
3. In the **Configuration** field, select a saved configuration.
4. Click **Test**.

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

   You need to use the admin credentials to view the settings.
6. Click **OK** to close the Test Settings window.

## Publishing the configuration settings

### Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Dynamic Configuration** > **Configuration**.

   The system displays the Configuration page.
3. In the **Configuration** field, select a saved configuration.

4. At the bottom of the page, click **Publish**.

   The system displays the Publish/Delete Settings window.

5. 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.
6. 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.
7. 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.
8. 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.
9. To apply the global settings to all users, select the **Global settings will be applied to all users** check box.
10. Click **Publish**.

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

# Importing 46xxsettings file

## About this task

You can import a 46xxsettings file as test configuration to check whether the parameters in the file are supported.

## Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Dynamic Configuration** > **Configuration**.

   The system displays the Configuration page.

3. Click **Import**.

   The system displays the Import 46xxsettings Configuration page.

4. Click **Browse** and select the 46xxsettings file that you want to test.

   If the 46xxsettings file has IF/GOTO statements, the system displays additional fields.

5. If the 46xxsettings file has IF/GOTO statements, select appropriate variables to process the IF/GOTO label conditions.
6. Click **Import**.

   The system imports the values and displays the results of the import. You can then save or publish the imported values.

## Retrieving configuration settings for a user

### About this task

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

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

### Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Dynamic Configuration** > **Configuration**.

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

      The system displays the configuration settings of the user.

# Administering the default configuration

### About this task

Using the Default page, you can maintain internal Dynamic Configuration parameters.

### Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Dynamic Configuration** > **Default**.

   The system displays the Defaults page.
3. Modify the default configuration settings.
4. Click **Save**.

**Related links**

Defaults field descriptions on page 59

## Defaults field descriptions

| Name | Description |
|---|---|
| **Allow passwords** | Specifies that the user can log in to the device with the stored password on the server.<br>• If you select the check box, the Dynamic Configuration displays the SIPHA1 and SIPPASSWORD settings. The Avaya UC clients use these SIP credentials for Unified login.<br>• If you clear the check box, the Dynamic Configuration does not display the SIPHA1 and SIPPASSWORD 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.<br>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.<br>• If you select the check box, you can view the obscured settings (OBSCURE_PREFERENCES) in the Dynamic Configuration response.<br>The value of OBSCURE_PREFERENCES and LOCKED_PREFERENCES are the same.<br>• If you clear the check box, the system hides the obscured settings (OBSCURE_PREFERENCES) in the Dynamic Configuration response. |
| **Scopia synchronization interval** | Specifies the days for synchronizing the settings of the Scopia server configurations. The system performs periodic synchronization to retrieve a list of users and their virtual rooms from the Scopia server.<br>The Dynamic Configuration service prints the virtual room number for the user. For example: SET CONFERENCE_VIRTUAL_ROOM 453<br>The days can be from 1 through 10. |
| **Scopia server** | Specifies the Scopia server URL. This field is specific to the Scopia server. |

| Name | Description |
|---|---|
| | The default Scopia Management XML API ports are:<br>• For TCP: 3336.<br>For example: http://myscopia.mgmt.avaya.com:3336<br>• For TLS: 3346.<br>For example: https://myscopia.mgmt.avaya.com:3346<br>For establishing a TLS connection, Avaya Aura® Device Services and Scopia must be configured with same trusted System Manager certificates. For more information, see *Administrator Guide for Avaya Scopia® Management for Aura Collaboration Suite* and *Avaya Scopia® Management XML API Reference Guide* on the Avaya Support website. |

| Button | Description |
|---|---|
| **Save** | Saves the default configuration settings. |
| **Get Status** | Gets the connection status of the Scopia server. |
| **Cancel** | Resets any changes made on the page. |

**Related links**

Administering the default configuration on page 58

# Split Horizon DNS Mapping overview

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.

**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 IP addresses of the Presence server 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.

**Related links**

Mapping IP address to FQDN on page 61
Enabling Split Horizon DNS mapping on page 61
Split Horizon DNS Mapping field descriptions on page 62

# Mapping IP address to FQDN

## About this task

Use this procedure to map the IP address to 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 interface.
2. In the left navigation pane, click **Dynamic Configuration** > **DNS Mapping**.

   The system displays the Split Horizon DNS Mapping page.
3. Click **Add**.

   The system displays a new row to add the IP address and FQDN.
4. In the **IP address** field, type the IP address of the server or URL to which the client will connect.
5. In the **Fully Qualified Domain Name** field, type the FQDN of the server or URL to which the client will connect.
6. Click **Save**.

**Related links**

Split Horizon DNS Mapping overview on page 60

# Enabling Split Horizon DNS mapping

## Procedure

1. Log on to the Avaya Aura® Device Services interface.

2. In the left navigation pane, click **Dynamic Configuration** > **DNS Mapping**.

   The system displays the Split Horizon DNS Mapping page.

3. Select the **Enable Split Horizon DNS Mappings** check box.

**Related links**

Split Horizon DNS Mapping overview on page 60

## 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. |

**Related links**

Split Horizon DNS Mapping overview on page 60

# Bulk Import overview

With Bulk Import, 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 the values and the example for specifying the bulk settings:

| Settings | Description |
|---|---|
| CATEGORY | Indicates the high-level category to which the particular setting belongs. The categories are:<br>• USER<br>• GLOBAL<br>• GROUP |

| Settings | Description |
|---|---|
| | • PLATFORM<br>• EXCEPTION |
| {SUB-CATEGORY} | Indicates the name or ID of the particular object (user id, group name, platform name) for which the setting value will be inserted, updated, or deleted.<br>• For the GROUP category, the sub-category is a group name. You can retrieve the group name from LDAP Server.<br>Example: GROUP;Group 1;SUPPORTEMAIL;admin@mysite.com<br>• For the USER category, the subcategory is a user name. The setting name is `ESMUSERNAME`.<br>Example: USER;user1@mysite.com;CESUSERNAME;user1@mysite.com<br>• For the PLATFORM category, the subcategory is a platform name. The options are **Mac**, **Windows**, **Android**, and **iOS**.<br>Example: PLATFORM;Windows;APPCAST_URL;https://appcast.mysite.com<br>• For the GLOBAL category, there is no sub-category. The format is: `{CATEGORY};{SETTING_NAME};{SETTING_VALUE}`<br>Example: GLOBAL;CESSECURE;1<br>• For the EXCEPTION category, the format is: `{CATEGORY};{SOURCE};{EXCEPTION_CONDITION_NAME};{EXCEPTION_CONDITION_VALUE};{SETTING_NAME};{SETTING_VALUE}`.<br>Where:<br>- {SOURCE} is SMGR.<br>- {EXCEPTION_CONDITION_NAME} is the Home location.<br>- {EXCEPTION_CONDITION_VALUE} is the location name.<br>- {SETTING_NAME} is the name of the setting.<br>- {SETTING_VALUE} is the value of the setting.<br>Example: EXCEPTION;SMGR;Home Location;location 1;PHNLDLENGTH;5 |
| **Note:**<br>To delete a setting from the configuration service, append DELETE instead of {SETTING_VALUE}.<br>Example: USER;user1@mysite.com;CESUSERNAME;DELETE | |

## Related links

Importing configuration settings on page 64
Bulk Import field descriptions on page 64

# Importing configuration settings

### Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Dynamic Configuration** > **Bulk Import**.

   The system displays the Bulk Import page.
3. To import the settings, do one of the following:
   - In the text box, type the entry in each line in the following format and click **Import**.

     ```
     {CATEGORY}
     ;
     {SUB-CATEGORY}
     ;
     {SETTING_NAME}
     ;
     {SETTING_VALUE}
     ```
   - Click **Choose File** to select a file from the local system and click **Import**.

     The file must be in the CSV format.

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

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

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

### Related links

Bulk Import overview on page 62

# 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** | Selects a file in the .csv format for importing the bulk configuration settings. |

| Button | Description |
|---|---|
| **Import** | Imports the added entry or the file and displays the status at the top of the page.<br>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.` |
| **Reset** | Resets the added entry and clears the text box. |
| **Refresh status** | Refreshes the import status. |

### Related links

Bulk Import overview on page 62

# Chapter 6: Configuring Web Deployment

## Web Deployment service overview

Using the Web Deployment service, you can provide appcast for the clients. Currently, you can create appcast only for the Avaya Equinox™ desktop clients. On the Web Deployment page, you can add, edit, or delete an appcast item from the appcast table that is at the bottom of the page.

The Web Deployment service supports the upload and download of the client installer that has software update files. The system creates the upload folder automatically at the time of deployment or upgrade. The administrator can also store any files that are necessary for customer to download. The customer can download the necessary files from `https://<aads_server_address>:8445/acs/resources/webdeployment/downloads/<file_name_with_extension>`. The upload service operates from the directory `/opt/Avaya/DeviceServices/ClientInstallers/`.

Example of the Upload URL: `<https://IP address>:8445/admin/upload`

Example of the Download URL: `<https://IP address>:8445/acs/resources/downloads/>`.

### Settings for receiving the updates from a client installer

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

- APPCAST_ENABLED
- APPCAST_CHECK_INTERVAL
- APPCAST_URL

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

The APPCAST_URL must be set to `https://<IP address of the AADS Server>:<8443>/acs/resources/webdeployment`

## Creating an upload folder

### Procedure

1. On the SSH terminal, log in as `admin`.

2. To create a client installer directory, type `sudo mkdir /opt/Avaya/DeviceServices/ClientInstallers`.
3. To change the owner, type `sudo chown ucapp:ucgrp /opt/Avaya/DeviceServices/ClientInstallers`.

# Configuring software update deployment

### About this task

Use this procedure to upload and download the client installer for web deployment.

### Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Web Deployment** > **Deployment**.

   The system displays the Software Update Deployment page.
3. In the **Title** field, type the name of the updates or appcast for the client installer.

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

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

   The system displays: `Avaya Communicator Windows Version 2.0: Critical update`
4. In the **Description** field, type the description of the client installer updates.

   For more information, see the Release Note for the new client installer.
5. In the **Version** field, type the version detail of the Avaya Communicator client release.
6. In the **OS** field, select one of the platforms of the Avaya Communicator client release:
   - Windows
   - Macintosh
7. In the **File** field, click **Choose File** to upload a plug-in file (Avaya Communicator client installer) from the local system.

   The file must be of the `.exe`, `.msi`, or `.dmg` format. Maximum size for uploading the client installer is 100 MB.

   The upload service accepts alphanumeric characters, white spaces, dots, minus, and square brackets.

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

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

   The system displays a pop up to specify the user credentials to upload the client installer and a confirmation dialog box to indicate the upload status.
9. 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 credential for client authentication.
10. Click **Save** to save the settings.

    the system populates the data in the table at the bottom of the page with the details of **Product Title**, **Description**, **Version**, **Publish Date**, **OS**, **Language**, **Type**, and **Download URL**. To edit or delete a specified setting, you can double-click to select an entry.

# Editing an appcast item

### Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Web Deployment** > **Deployment**.

   The system displays the Software Update Deployment page.
3. On the bottom of the Software Update Deployment page, double-click an entry in the table.

   The system displays the Edit appcast item page.
4. Edit the settings that you want to change.
5. Click **Save**.

   The system populates the updated data in the table at the bottom of the page.

# Deleting an appcast item

### Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Web Deployment** > **Deployment**.

   The system displays the Software Update Deployment page.

3. On the bottom of the Software Update Deployment page, click an entry in the table.

   The system displays the Edit appcast item page.
4. Click **Delete**.

   The system displays the Delete item page.
5. Click **Yes**.

# Chapter 7: Administering Session Manager for clustering

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

Repeat these steps for all Avaya Aura® Device Services nodes in the cluster.

### Before you begin

Deploy the Avaya Aura® Device Services OVA.

**Note:**

Avaya Aura® Device Services is available only with Avaya Equinox™ 3.0.

### Procedure

1. On the System Manager web console, click **Services** > **Inventory**.
2. In the left navigation pane, click **Manage Elements**.
3. On the Manage Elements page, click **New**.

   The system displays the New Elements page.
4. In the **General** section, from the **Type** field, select **Avaya Aura Device Services**.

   The system refreshes the page and displays the New Avaya Aura Device Services page.
5. On the **General** tab, perform the following:
   a. In the **Name** field, type the name of the Avaya Aura® Device Services server.
   b. In the **Description** field, type the description of the Avaya Aura® Device Services server.
   c. In the **Node** field, type the IP of the Avaya Aura® Device Services server.
6. On the **Attributes** tab, perform the following:
   a. In the **Login** field, type the admin login name to access the Avaya Aura® Device Services server.
   b. In the **Password** field, type the admin password to access the Avaya Aura® Device Services server.

c. In the **Confirm Password** field, retype the admin password to access the Avaya Aura® Device Services server.

d. In the **Version** field, type the version of the Avaya Aura® Device Services server.

e. In the **Location** field, type the location name of the Avaya Aura® Device Services server.

7. Go back to the General tab.

**Important:**

Access profiles of type GRCommunication and TrustManagement are available by default.

8. Select the TrustManagement access profile, and click **Edit**.
9. In the **Host** field, type the FQDN or IP address of the Avaya Aura® Device Services server.
10. Leave the **Container Type** field blank.
11. Leave the other fields unchanged at default values.
12. Click **Save**.

To enable SSO login, you must add an access profile of type EMURL. Steps 13a to 13k show how to add an access profile of type EMURL.

13. To add an EMURL access profile, on the **General** tab, in the Access Profile section, perform the following:

a. Click **New**.

b. In the Application System Supported Protocol section, in the **Protocol** field, click **URI**.

c. In the Access Profile Details section, in the **Name** field, type a name for the access profile.

d. In the **Access Profile Type** field, click **EMURL**.

e. In the **Protocol** field, click **https**.

f. In the **Host** field, type the Avaya Aura® Device Services server FQDN.

g. In the **Port** field, type `8445`.

h. In the **Path** field, type `/admin`.

i. In the **Order** field, retain the default value.

j. In the **Description** field, type a description of the access profile.

k. Click **Save**.

14. Click **Commit**.

## Next steps

Go to the System Manager home page and click **Device Services** in the Elements section.

The Device Services page displays the Avaya Aura® Device Services element you added. After Avaya Aura® Device Services installation is complete, you can click the name of the Avaya Aura® Device Services element to open the Avaya Aura® Device Services home page.

# Pairing Session Manager with an Avaya Aura® Device Services node

### About this task

You can pair a Session Manager instance to an Avaya Aura® Device Services node while adding a Session Manager instance or after adding the Session Manager instance using the **Edit** button.

Repeat these steps for all Avaya Aura® Device Services nodes in the cluster.

For example, for a Session Manager cluster with two nodes, SM01 and SM02, to deploy an Avaya Aura® Device Services cluster with two nodes, AADS01 and AADS02, you must pair:

- SM01 with AADS01
- SM02 with AADS02

### Before you begin

Assign the Session Manager instance to a data center.

### Procedure

1. On the home page of the System Manager Web Console, in **Elements**, click **Session Manager** > **Session Manager Administration**.
2. On the Session Manager Administration page, click the **Session Manager** Instances tab.
3. In the **Session Manager Instances** section, select a Session Manager instance, and click **Edit**.

   The system displays the Edit Session Manager page.
4. From **Data Center**, select a data center if one is not already assigned.

   If you do not assign the Session Manager instance to a data center, the system displays the following message: `Session Manager must be assigned to a Data Center to pair with an Avaya Aura Device Services Server.`
5. From **Avaya Aura Device Services Server Pairing**, select an Avaya Aura® Device Services server.

   When an AADS server is already paired with a Session Manager instance, the system does not display that Avaya Aura® Device Services Server in the **Avaya Aura Device Services Server Pairing** drop-down list.
6. Click **Commit**.

# Effect of Session Manager on Avaya Aura® Device Services

Session Manager can have one of the following Service States:

- Accept New Service: In this state, Session Manager accepts incoming calls.

  When Session Manager is in Accept New Service state, Avaya Aura® Device Services contact services works uninterrupted.

- Deny New Service: In this state, Session Manager denies any new call attempts and service requests.

  When Session Manager is in Deny New Service state, Avaya Aura® Device Services Contact Services do not work. Avaya Aura® Device Services is also placed in Deny New Service state and sends an HTTP/503 error for all add, update, and delete requests for contact service.

- Maintenance Mode: In this state, Session Manager is placed in a dormant state for maintenance.

  When Session Manager is in Maintenance state, Avaya Aura® Device Services Contact Services do not work. Avaya Aura® Device Services is also placed in Maintenance state and sends an HTTP/503 error for all add, update, and delete requests for contact service.

# Chapter 8: Avaya Aura® Device Services Cluster Monitoring and Management

## 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 interface.
2. In the left navigation pane, click **Cluster Configuration** > **Cluster Nodes**.

   The system displays the Cluster Monitoring and Management page.
3. Check the status of the Avaya Aura® Device Services nodes in the table.

   The table has the following column headers to display the status:

   - **Node Address**
   - **Status**
   - **Service Status**
   - **Singleton Services**

   Audits that run only on a single node are called singleton services.

**Related links**

[Cluster Nodes field descriptions](#) on page 74

## Cluster Nodes field descriptions

| Name | Description |
|---|---|
| **Virtual IP** | Displays the virtual IP address if a virtual IP address is configured. This is used as a load balancer node. |
| **Virtual IP Master** | Displays the virtual IP master node if a virtual IP address is configured. |

| Name | Description |
|---|---|
| **Virtual IP Backup** | Displays the virtual IP backup node if a virtual IP address is configured. |
| **Seed Node IP** | Displays the IP address of the seed node of the cluster. |

### Related links

Monitoring cluster nodes on page 74

# Chapter 9: Logs and Alarms

## Log management

The system stores the common log at `/opt/Avaya/DeviceServices/7.0.1.0.<build-number>/logs/AADS.log`.

You can view additional messages at `/opt/Avaya/DeviceServices/7.0.1.0.<build-number>/tomcat/8.0.24/logs/catalina`. These messages can be the logs generated during the start of Avaya Aura® Device Services.

## Monitoring the Avaya Aura® Device Services logs

### About this task

You can monitor the `AADS.log` file in runtime using the **`tail`** command.

### Procedure

1. On the SAT terminal, log in to Avaya Aura® Device Services.
2. Run the command: **`tail -f /opt/Avaya/DeviceServices/7.0.1.0.<build-number>/logs/AADS.log`**.

   The system displays the logs generated during run time.

## Setting up the log level

### About this task

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

### Procedure

1. Log on to the Avaya Aura® Device Services interface.
2. In the left navigation pane, click **Log Management** > **Log Level**.

   The system displays the Adjust Service Logging Level page.

3. In the **Logger** field, select one of the following:
   - Avaya Aura Device services Logs: Collects the logs generated by the Avaya Aura® Device Services server.
   - Client Application Service Logs: Collects the logs generated by the client application.
   - System Logs: Collects all the system logs.
   - All Logs: Collects all the logs generated by the Avaya Aura® Device Services server and the system.
4. In the **Current logging level** field, select one of the following:
   - 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: option provides detailed logs. The Dynamic Configuration and Web Deployment services use this information for debugging purposes, such as, method started and method finished.

     **Warning:**

     Setting logs at FINE logging level can affect system performance.
   - FINEST: provides very detailed logs on frequent events. These logs can impact server performance.

     **Warning:**

     Setting logs at FINEST logging level can affect system performance.
5. Click **Save**.

# Alarms

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

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

**Table 1: Avaya Aura® Device Services alarms**

| 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 |

| Alarm description | Severity | Event code | SNMP OID |
|---|---|---|---|
| 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 |
| 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 |
| AADS Multisite Adapter Successfully connected to remote site(s) | major | OP_AADS-00085 | .1.3.6.1.4.1.6889.2.89.0.85 |
| AADS Multisite Adapter Cannot connect to remote site(s) | major | OP_AADS-00084 | .1.3.6.1.4.1.6889.2.89.0.84 |
| 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 |

| Alarm description | Severity | Event code | SNMP OID |
|---|---|---|---|
| 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 |
| 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 |

| Alarm description | Severity | Event code | SNMP OID |
|---|---|---|---|
| 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 |
| 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 |

| Alarm description | Severity | Event code | SNMP OID |
|---|---|---|---|
| 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 |
| 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 |

| Alarm description | Severity | Event code | SNMP OID |
|---|---|---|---|
| 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 |
| Test alarm | minor | OP_AADS-00001 | .1.3.6.1.4.1.6889.2.89.0.1 |

**Related links**

Setting up the log level on page 76

# Setting up Serviceability Agents for alarms

## Before you begin

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

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

Set up an SNMP target profile from **Services** > **Inventory** > **Manage Serviceability Agents** > **SNMP Target Profiles**.

## About this task

To receive Avaya Aura® Device Services alarms in System Manager, you must set up Serviceability Agents.

## Procedure

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

   System Manager is now ready to receive alarms from Avaya Aura® Device Services.

# Chapter 10: Client Certificate Policy

Avaya Aura® Device Services and Avaya Aura® Device Services clients can process a certificate to establish a secure connection. As per your requirement, you can choose how the server validates certificates for Avaya Aura® Device Services clients. The validation of certificates are implemented at the Nginx level and based on the client certificate policy configuration, Nginx will respond with the error code or a success response.

**Note:**

Changing the certificate setting may affect client's ability to connect to Avaya Aura® Device Services.

## Configuring Client Certificate Policy through Avaya Aura® Device Services web interface

### Procedure

1. Log on to the Avaya Aura® Device Services web interface.
2. In the navigation pane, click **Client Administration** > **Client Settings**.

   The system displays the Client-Device Certificate Policy page.
3. To set the Client Certificate Policy for REST request, in the **REST** field, click the type of setting you want to use.
4. To set the Client Certificate Policy for the Admin UI (OAMP), in the **OAMP** field, click the type of setting you want to use.
5. Click **Save**.

## Client-Device Certificate Policy field descriptions

| Name | Description |
|---|---|
| **REST** | Specifies certificate processing options for REST requests. |

| Name | Description |
|---|---|
| | The options are:<br>• **NONE**: The server does not check for a certificate. The connection is established with or without a valid certificate.<br>• **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`.<br>• **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`.<br>• **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`.<br>The default value is: **OPTIONAL**. |
| **OAMP** | Specifies certificate processing options for OAMP.<br>The options are:<br>• **NONE**: The server does not check for a certificate. The connection is established with or without a valid certificate.<br>• **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`.<br>• **OPTIONAL_NO_CA**: The server requests a certificate. The connection is established with any valid certificate even if the CA is untrusted, but the process stops if a client provides an invalid certificate, and the system returns the error code `HTTP 400`.<br>• **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`.<br>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. |

# Configuring Client Certificate Policy through CLI

## About this task

You can use this procedure if you accidentally changed the admin interface (OAMP) client certificate policy and are no longer able to access the system interface. To change the certificate, you must access the Avaya Aura® Device Services seed node. Follow the procedure to change the setting through CLI.

## Procedure

1. On the SSH terminal, log in as admin.
2. Type one of the following:
   - To change the setting to **None**, type `sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/misc/clitool-acs.sh clientCertificateVerificationConfig oampGuiClient off`.
   - To change the setting to **Optional**, type `type sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/misc/clitool-acs.sh clientCertificateVerificationConfig oampGuiClient optional`.
   - To change the setting to **Required**, type `sudo /opt/Avaya/DeviceServices/<version>/CAS/<version>/misc/clitool-acs.sh clientCertificateVerificationConfig oampGuiClient on`.
3. After running the command, wait for a few minutes to reflect the changes.

# Chapter 11: Troubleshooting

## DRS remains in Ready to Repair state

### Cause

Tomcat must restart to register the DRS URL.

### Solution

Restart Tomcat by using the AADSTomcat restart service.

Restarting tomcat changes the DRS state to repairing, synchronizing, and then synchronized.

## DRS remains in repairing state for a long time

### Cause

Avaya Aura® Device Services logs are set in FINESTlevels, because of which huge nginx logs are created during drs process, thereby causing connection timeouts.

### Solution

1. Change the log level of Avaya Aura® Device Services log to WARN level.
2. From System Manager, mark the node for repair again.

   After the node is synchronized, you can change the log level back to FINEST.

**Related links**

Setting up the log level on page 76

## DRS remains in not polling state

### Cause

System Manager and Avaya Aura® Device Services are not in the same DNS or the `/etc/hosts` file of System Manager.

If the FQDN is resolved, you need not use host files and the DRS not polling error does not occur.

### Solution

1. If the System Manager host file does not have the Avaya Aura® Device Services IPs, add the IPs to the `/etc/hosts` file, and vice versa.
2. Log in to Avaya Aura® Device Services.
3. Go to `/opt/Avaya/DeviceServices/<version>/CAS/<version>/bin` and run the `configureAADS.sh` script.
4. Reconfigure System Manager details again and wait till the DRS configure process is complete.

## 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 while using an earlier version.

If you are using an older version of PuTTY, you might receive an `Access Denied` error when pasting the response code.

### Solution

Update PuTTY to the latest version.

## ESG cannot connect to Avaya Aura® Device Services when REST Certificate Policy is set to none

Occurs in a deployment with Avaya Aura® Device Services and Avaya Aura® Web Gateway, if both Avaya Aura® Device Services Web deployment feature for desktops, and WebRTC calls feature with Avaya Aura® Web Gateway is being used.

### Solution

Set the certificate validation policy in Avaya Aura® Device Services Admin GUI to Optional. Do not set the certificate validation policy to none.

Web Deployment binaries for Avaya Equinox™ client for Windows and Mac must be moved to another web server or follow the instructions below to add the binaries to Avaya Aura® Device Services web server on a unchallenged web port. The client cannot send certificates to Avaya Aura® Device Services WebDeployment service in this release.

**Note:**

Web Deployment feature is only accessible within the Enterprise network or through VPN.

# Running patch to allow Avaya Equinox™ for Windows to reach Web Deployment service

## About this task

For software updates through Avaya Equinox™ for Windows client, you must apply a patch by following the instructions in this section. The patch opens port 8442 for Web deployment service and sets up port 8442 to pass web deployment requests without certificate validation.

**Important:**

You must use this procedure only if you have Avaya Equinox™ for Windows clients and ESG servers in your environment.

If you have only Avaya Aura® Device Services and Avaya Equinox™ for Windows clients in the network, you must set the REST and OAMP fields on the **Client Administration** > **Client Settings** screen to None.

You can use the patch with the following arguments:

- enable: to apply the workaround to allow Avaya Equinox™ for Windows to reach Web Deployment service
- disable: to revert the workaround to allow Avaya Equinox™ for Windows to reach 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.

## Procedure

1. Go to `/opt/Avaya/DeviceServices/version/CAS/version/misc/`.
2. Type `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/
   7.0.1.1.105/nginx/1.8.0-1/conf/nginx.conf
   acs-nginx-webdeployment-8442.conf will be added now
   iptables rule will be added now
   iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
   2017-01-24_12:17:36 Reloading Nginx .....................  [  OK  ]
   ```

   After running the patch, you must download URL and appcast URL to use port 8442.
3. Log in to the Avaya Aura® Device Services administration user interface.
4. In the navigation pane, click **Web Deployment** > **Deployment**.

   The system displays the Software Update Deployment page.
5. Change the Download URL port for Appcast to 8442.

   For example, https://<AADS FQDN/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/IP Address>:8442/acs/resources/webdeployment

# Failed to generate new private key

### Condition

Avaya Aura® Device Services configuration utility closes abruptly while configuring the SSH/RSA Public/Private keys.

### Cause

The `/home` directory is full. Therefore, the system is not able to create `/authorized_keys` file and the system displays a disk space check warning in the log file.

### Solution

Clean up the `/home` directory.

# Slow Avaya Aura Device Services performance

### Cause

The network latency between all Avaya Aura® Device Services and their respective Session Managers is more than 5 ms.

### Solution

The network latency between all Avaya Aura® Device Services and their respective Session Managers must be less than 5 ms.

# Unable to access administration UI when the primary node SM is nonoperational

In a cluster, if the SM associated with the primary AADS node is nonoperational, the AADS administration UI is unavailable.

### Solution

Administrator must use the FQDN for the other nodes in order to access AADS admin UI, when the primary node is nonoperational.

# Chapter 12: Resources

## Documentation

See the following related documents at http://support.avaya.com.

| Title | Use this document to: | Audience |
|---|---|---|
| Implementing | | |
| *Deploying Avaya Aura® Device Services* | Deploy Avaya Aura® Device Services. | Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel |
| *Deploying Avaya Aura® Session Manager* | Deploy the Session Manager OVA. | Sales Engineers, Solution Architects, Implementation Engineers, Support Personnel |
| Administering | | |
| *Administering Avaya Aura® Device Services* | Administer Avaya Aura® Device Services. | Sales Engineers, Solution Architects, Support Personnel |
| *Administering Avaya Aura® Session Manager* | Administer the Session Manager interface. | Sales Engineers, Solution Architects, Support Personnel |

**Related links**

Finding documents on the Avaya Support website on page 90

## Finding documents on the Avaya Support website

### About this task

Use this procedure to find product documentation on the Avaya Support website.

### Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.

3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

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

**Related links**

Documentation on page 90

# Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

## About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

## Procedure

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

**Note:**

Videos are not available for all products.

# Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

# Index

## M



## N



## O



## P



## R



## S



## T



## V



## W