Administration using Avaya Fabric Orchestrator

Release 1.0
NN48100-600
Issue 01.02
November 2015

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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

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

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

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A 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. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING 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.

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

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

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").

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

The following applies 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

Customer acknowledges and agrees that it is responsible 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, 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 concepts, operations, and tasks related to the management features of theAvaya Fabric Orchestrator (AFO). This guide also describes additional administrative tasks such as backups, software updates, preferences, and troubleshooting.

Related resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com.

Document title	Use this document for:	Audience
Avaya Fabric Orchestrator Solution Description, NN48100–100	Description of each verified reference configuration.	System administrator
Deploying Avaya Fabric Orchestrator, NN48100–101	Installing, configuring, initial administration, and basic maintenance checklist and procedures.	System administrator
Getting Started and Locating the latest software and Release Notes for Avaya Fabric Orchestrator, NN48100–102	Locating the latest software and product release notes.	System administrator
Network Monitoring using Avaya Fabric Orchestrator, NN48100–500	Monitoring the managed objects in AFO.	System administrator
Network Configuration using Avaya Fabric Orchestrator, NN48100–501	Configuring and managing Avaya Enterprise family of devices from discovered network.	System administrator

Table continues…

Document title	Use this document for:	Audience
Bulk Device Configuration Management using Avaya Fabric Orchestrator, NN48100–502	Performing a variety of management tasks across multiple device types using a web-based interface.	System administrator
Virtualization Configuration using Avaya Fabric Orchestrator, NN48100–503	Connecting the vCenter server to AFO, to help the data center administrator to configure the network changes that apply to the data center.	System administrator
IP Flow Configuration using Avaya Fabric Orchestrator, NN48100–504	Collecting and analyzing IP flows from IPFIX-, NetFlow v5-, and NetFlow v9- enabled devices.	System administrator
Administration using Avaya Fabric Orchestrator, NN48100–600	AFO System administration procedures.	System administrator
Avaya Fabric Orchestrator Traps and Trends Reference, NN48100–700	Viewing a list of supported traps and trends.	System administrator
Avaya Fabric Orchestrator Supported Devices, Device MIBs, and Legacy Devices Reference, NN48100–701	Confirming support for devices and MIBs.	System administrator

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com/.

Viewing Avaya Mentor videos

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

About this task

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

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.

Subscribing to e-notifications

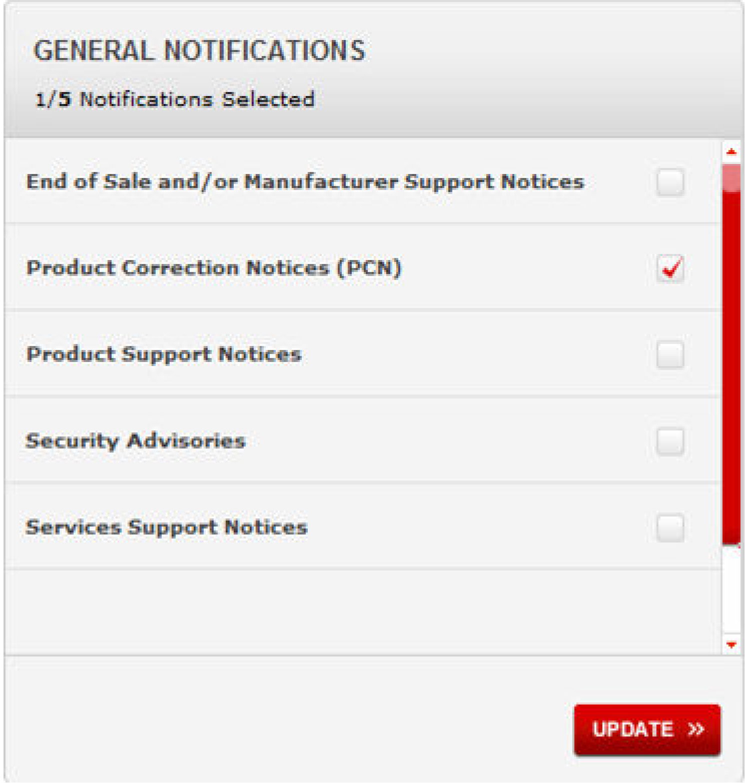
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Virtual Services Platform 7000.

Procedure

1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Under **My Information**, select **SSO login Profile**.
4. Click **E-NOTIFICATIONS**.
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.

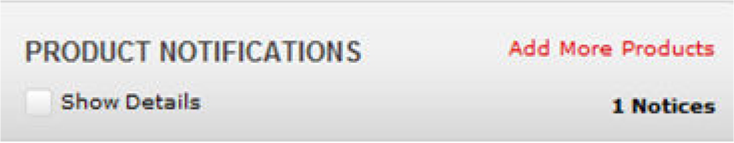


GENERAL NOTIFICATIONS

1/5 Notifications Selected

- End of Sale and/or Manufacturer Support Notices □
- Product Correction Notices (PCN) ☑
- Product Support Notices □
- Security Advisories □
- Services Support Notices □

6. Click **OK**.
7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.

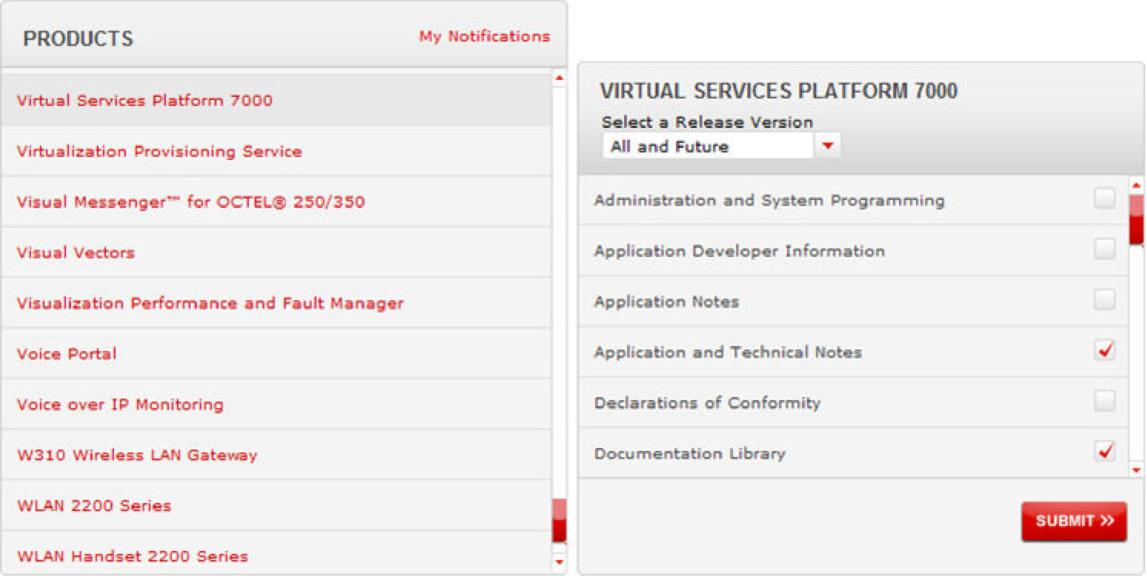


PRODUCT NOTIFICATIONS

□ Show Details

1 Notices

8. Scroll through the list, and then select the product name.
9. Select a release version.
10. Select the check box next to the required documentation types.



PRODUCTS

My Notifications

- Virtual Services Platform 7000
- Virtualization Provisioning Service
- Visual Messenger™ for OCTEL® 250/350
- Visual Vectors
- Visualization Performance and Fault Manager
- Voice Portal
- Voice over IP Monitoring
- W310 Wireless LAN Gateway
- WLAN 2200 Series
- WLAN Handset 2200 Series

VIRTUAL SERVICES PLATFORM 7000

Select a Release Version: All and Future

- Administration and System Programming □
- Application Developer Information □
- Application Notes □
- Application and Technical Notes ☑
- Declarations of Conformity □
- Documentation Library ☑

11. Click **Submit**.

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.

Chapter 2: New in this document

Administration using Avaya Fabric Orchestrator, NN48100–600 is a new document for Release 1.0 so all the features are new in this release. See *Avaya Fabric Orchestrator Release Notes* for a list of supported features.

Chapter 3: Avaya Fabric Orchestrator (AFO) Overview

The Avaya Fabric Orchestrator (AFO) is the next generation Management and Orchestration solution from Avaya. AFO creates an open framework for managing networking gear at a higher level of abstraction using Avaya Fabric Networking technology. This solution separates the control and data management planes of the network. AFO architecture is comprised of new and existing products intended to ease onboarding of users and devices to the network.

AFO is a single, pre-installed, easily deployable appliance with a web-based multi-user solution. AFO integrates all its tools in a single device. AFO includes a set of management features that helps lower the TCO, delivers automation, and simplifies operational processes. The following is a list of AFO management features:

Table 1: AFO network management applications

Application	Description	Features
AFO Configuration	Provides an intuitive interface to configure and manage the Avaya Enterprise family of devices from a discovered network.	• VLAN • MLT • Routing • VRF • Multicast • Fabric Connect • Fabric Extend • Multimedia • Trap/Log Registration • Security • Device Groups • File Inventory
AFO Bulk Provisioning	Performs a variety of management tasks across multiple device types using a web-based interface.	• Configuration Backup and Restore • Configuration Update Generator • Device Password Manager • Inventory

Table continues…

Application	Description	Features
		• Log Browser • Scheduler • Software Version Updater • TunnelGuard Distributor • Reports
AFO Monitoring	Monitors the managed objects in AFO, and reduces troubleshooting issues because of a more complete view of the network.	• Built-in monitoring for supported devices (Availability, KHI Bandwidth only) • Event-driven E-mail action • Event-driven scripting action • Built-in monitoring dashboard (view only) • Buit-in reports (view only) • PDF and Excel export of reports and trends • Basic enumerated scopes • Trap and Syslog viewers • Basic virtualization support (Hyervisor and VM discovery) • Advanced discovery (multi-vendor, non-Avaya L4/L7 software and applications • Advanced monitoring • Custom actions • Dashboards you can customize, and dashboard builder • Reports that you can customize, and reports builder • Advanced scopes • Network baselining
AFO IP Flow	Collects and analyzes IP flows from IPFIX-, NetFlow v5- and NetFlow v9-enabled devices. All management functions are provided through a Web-based user interface.	• Flows collection • Flows analysis by protocol and applications • PDF export to charts • Custom protocol monitoring • Custom application monitoring

Table continues…

Application	Description	Features
		• PDF, Excel, and CSV export of charts and data
AFO Virtualization	Connects the vCenter server to AFO Configuration to help the data center administrator configure the network changes that apply to the data center.	• Monitoring virtual infrastructure and provision network

AFO delivers enterprise-class reliability, efficiency, and scaling to mission-critical networks around the globe. Thus, significantly reducing the cost of managing networks.

Chapter 4: Administration tools

Administration tools overview

You can manage the Avaya Fabric Orchestrator (AFO) appliance and various features through the following administration tools:

- The AFO web interface
- The command line interface (CLI)

AFO web interface

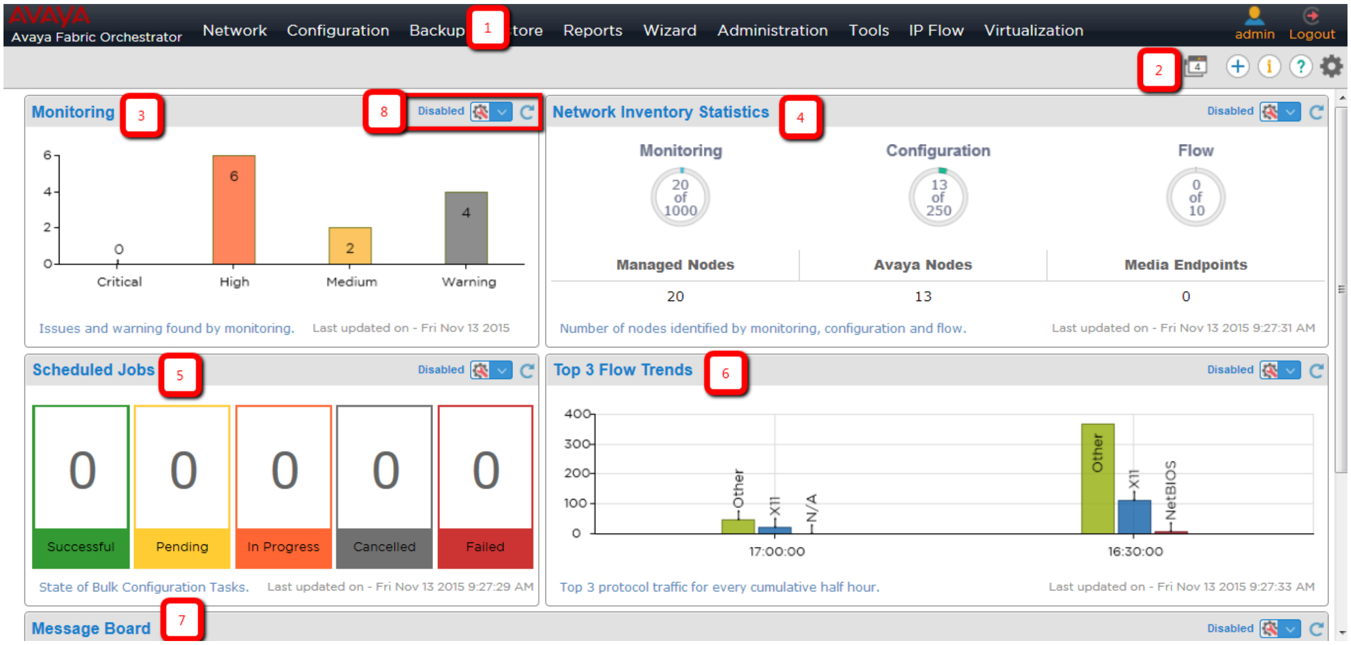
The AFO is designed to be viewed using Microsoft Internet Explorer, versions 10, 11, or Mozilla Firefox, versions 40, 41.AFO provides you with an improved user experience across all Avaya tools with data-driven menus for easy integration with current applications and future add-ons.

The Home page appears when you start AFO, and provides a real-time statistical view of the various applications integrated on the AFO in the form of portlets. The portlets are the dynamic components on AFO Home page that displays live feeds of the applications. Home page also provides shortcuts to common AFO tasks, and links to information.

You can use the Home page to determine the operating status of the various modules and applications in your AFO configuration.

You can return to the Home page at any time during your AFO session. To return to this page, click **Avaya Fabric Orchestrator** on the menu bar.

The following figure shows the overall sections of the AFO Home page:



Issues and warning found by monitoring. Last updated on - Fri Nov 13 2015

Number of nodes identified by monitoring, configuration and flow. Last updated on - Fri Nov 13 2015 9:27:31 AM

State of Bulk Configuration Tasks. Last updated on - Fri Nov 13 2015 9:27:29 AM

Top 3 protocol traffic for every cumulative half hour. Last updated on - Fri Nov 13 2015 9:27:33 AM

Figure 1: AFO Home page

Table 2: AFO Home page

No.	Name	Description
1	Menu bar	Provides the navigation options for AFO. The area at the top of the AFO window displays primary and secondary tabs that you accessed during the session; the tabs remain available until you close them. The following list gives the list of primary tabs: • Network • Configuration • Backup & Restore • Reports • Access Control • Wizard • Administration • Tools • IP Flow

Table continues…

No.	Name	Description
		• Virtualization
2	Quick access Toolbar	Provides quick access to commonly used AFO commands and displays the second level of items for an area of functionality. Quick access toolbar contains the following items: • Second level items for the selected primary tab • Tab Scope • Quick Links • Add-ons • About • Help • Preferences
3	Monitoring Portlet	Provides real-time statistical view of the issues and warning found by Avaya Fabric Orchestrator Monitoring.
4	Network Inventory Statistics Portlet	Provides network inventory statistics information of the number of nodes identified by Avaya Fabric Orchestrator Configuration, Avaya Fabric Orchestrator Monitoring, and Avaya Fabric Orchestrator IP Flow.
5	Scheduled Jobs Portlet	Provides the state of Bulk Configuration tasks.
6	IP Flow Trending Analysis Portlet	Provides the top three protocol traffic for every cumulative at half an hour interval.
7	Message Board	Provides the top 25 messages to get an overall health of the system.
8	Portlets Toolbar	Provides the quick access functionality for each portlets: • Refresh Now — Refresh the data feed in the portlet. • Refresh Interval — Disable the feed or schedule a refresh at regular intervals.

AFO web interface icons

The following table shows the common icons that appear on top of the AFO window:

Table 3: Common icons

Icon	Name	Description
1	**Tab Scope**	Provides a way to open and manage all the active tabs. Tap Scope displays a number that defines the number of opened tabs. In this example, it displays number one, as there is only one tab open. **Note:** You can open a maximum of 12 tabs at any given time. Tab Scope displays only the current tab and to access any other open tab, click tab scope and navigate.
+	**Add-ons**	Provides you a way to add, remove, or launch add-ons. Select the desired add-ons from the drop-down list: • ADS Gateway • ADS SLAMon
i	**About**	Provides the basic information about the application, license, and software lineup. Use the About icon to install certificates.
?	**Help**	Displays the help page.
⚙	**Preferences**	Provides you a way to configure system and application settings.
Logout	**Logout**	Use Logout to exit from the application.

Logging on to the AFO web interface

About this task

Use this procedure to log on to the Avaya Fabric Orchestrator (AFO) web interface for the first time.

Before you begin

Ensure that you have:

- Installed and configured the AFO appliance.
- A computer with a supported web browser and access to the network where the AFO appliance is installed.
- The MSC server Fully Qualified Domain Name (FQDN) details.

Procedure

1. On the web browser, enter the MSC server URL `https://<Fully Qualified Domain Name>`.
2. In the **User ID** field, enter the default user name `admin`.
3. In the **Password** field, enter the default password `admin123`.
4. Click **Log On**.

   The system validates the user name and password with the AFO user account. Depending on the validity, the system displays one of the following screens:

   - If the user name and password match, the system displays the AFO web interface with the AFO *version_number*. The AFO web interface displays the menu bar. The menu bar provides access to shared services to perform various operations that AFO supports. The tasks you can perform depends on your user role.
   - If the user name and password does not match, AFO displays an error message and prompts you to re-enter the user name and password.

Next steps

- Change the default password.

✱ **Note:**

You must change the password when you log on to the system using the default password for the first time.

The password must contain a combination of alphanumeric and special characters.

Changing the password

About this task

Use this procedure to change the default AFO web-interface password.

❗ **Important:**

You must change the password when you log on to the system using the default password for the first time.

Before you begin

Ensure that you have:

- Installed and configured the AFO appliance.

- A computer with a supported web browser and access to the network where the AFO appliance is installed.
- The MSC server Fully Qualified Domain Name (FQDN) details.

Procedure

1. On the web browser, enter the MSC server URL `https://<Fully Qualified Domain Name>`.
2. On the AFO login page, click **Change Password**.

   The Password change page is displayed.
3. In the **User ID** field, enter the user name.
4. In the **Current password** field, enter the current password.
5. In the **New password** field, enter the new password.
6. In the **Confirm new password** field, re-enter the new password.
7. Click **Save** to change the password.

Next steps

Install AFO certificates.

AFO Command Line Interface

You can use the AFO command-line interface (CLI), a text-based interface, to administer and use some of the AFO key features. The CLI of the AFO provides a number of commands to perform the administrative and troubleshooting tasks. If the AFO web interface is unavailable for some reason, you can still use the AFO CLI to continue using the AFO features.

Through the AFO CLI, you can:

- Perform a factory reset
- View the hardware resource usage
- Perform AFO health check
- Start, stop, or restart the application service
- Update and edit the network configuration
- View the AFO HostID

Note:

You must use the AFO CLI to perform all the troubleshooting related tasks for AFO.

CLI commands for AFO

The following table lists the CLI commands available through CLI for AFO:

Command	Description	Syntax
`Factory reset`	Allows you to re-deploy AFO services on the server.	`afo-factory-reset`
`Resource usage`	Displays the current CPU and memory usage of each virtual machine.	`afo-resource-usage`
`Health check`	Allows you to check the status of the applications running on each virtual machine.	`afo-health-check`

AFO **`service`**	Allows you to easily stop, start, or restart the application service.	• To view the help menu
		`afo-service –help`
		• To restart an application service on a particular VM
		`afo-service -action restart -serviceid <service>`
		• To view the status of the application service on multiple VMs
		`afo-service -action status -serviceid <service 1> <service 2>`
		• To view the status of the application service on all the VMs
		`afo-service -action status -serviceid all`

AFO **`network change`**	Allows you to update and change the AFO network details post deployment. **Note:** It takes approximately 45 minutes to complete the configuration.	`afo-network-config`
AFO **`network information`**	Displays the hostname and IP address of all the virtual machines that are configured on AFO.	`afo-cluster-info`
AFO **`HostID`**	Provides the HostID for generating an AFO license.	`afo-hostid`

Chapter 5: Password and security policies

Password aging policy enforcement

The password aging policy has the following time-based password thresholds:

- Minimum password age
- Password expiration warning
- Password expiration period

The following table describes the password aging policy threshold rules and limitations after the user logs on to AFO.

Password threshold	Rules and Limitations
Minimum password age	You need to meet the minimum password age criteria before resetting the password. By default, minimum password age is set to one day. ✱ **Note:** You cannot change the password within or before that time.
Password expiration warning	You receive a password expiration warning during all the seven days before the password expires. ✱ **Note:** You cannot change the already expired password.
Password expiration period	Password expires in 90 days.

Password strength policy enforcement

The password strength policy that you as a system administrator defines enforces the following constraints:

- Passwords must have at least 8 characters.
  - The default is one lowercase character and one uppercase character, one numeric character, and one special character. The sum cannot exceed the minimum total length.

- Passwords must contain a combination of the following characters: a-z,A-Z,0-9,{}|()<>,/.=[]^_@!$%&-+":?`\;

Note:

When you enable the password strength policy, if the password does not meet the password strength policy, the system rejects the password.

Chapter 6: User management and Role Based Access Control

This chapter provides information about managing users, how to add, modify, or delete user accounts from the system. It also defines role-based access control (RBAC) authorization rules by creating new roles, modifying or deleting existing roles; to limit access to the AFO elements and permissions in those elements.

Managing roles

This section provides information about managing user roles. You can perform various Role Based Access Control (RBAC) tasks required to manage roles within the AFO. You can add or delete a role name, provide group-level authentication functions and element permissions.

Roles management tasks can be performed in **Administration** > **Roles**.

Role Based Access Control

In AFO, you require appropriate permissions to perform any task. The administrator grants permissions to users by assigning appropriate roles. The Role Based Access Control (RBAC) in AFO supports two types of roles:

- Built-in
- Custom

Using these roles, you can gain access to various elements with specific permission mappings. Built-in roles are the default roles that AFO provides. You can assign these roles to users, but you cannot delete these roles or change the permission mappings in the built-in roles. Built-in roles provide authorization to users for performing common administrative tasks.

Built-in roles

By default AFO will have the following built-in roles:

- AFO System Administrator
- AFO Network Administrator
- AFO Network Operator

These Role consist of one or more elements, with each element having different set of permissions. The following table specifies the permissions mapped to the built-in roles:

Role Name	Element Mapping	Role Permission Assigned
AFO System Administrator	AFO Primary Roles	Read-Write (Modify)
	AFO Configuration Services	Modify for all managers
	AFO Administration Services	Access AFO maintenance services
AFO Network Administrator	AFO Primary Roles	Read-Write (Modify)
	AFO Configuration Services	Read-Write (Modify) for each configuration component for all managers
AFO Network Operator	AFO Primary Roles	Read only (View)
	AFO Configuration Services	Read-Write (View) for all managers

Custom roles

On the **Roles** Web page you can create a custom role that maps to specific elements of different type and specify customized permissions for those elements. You can create custom roles for any user whose role is not authorized on one or more individual elements of any element type.

You can assign the roles that you created to users to perform specific tasks on an element. For example, a custom role that you create for a single element can only perform specific tasks on that element. There is a specific permissions set that defines what this role allows you to do on that element.

You can also define roles that apply to how elements and element types are hierarchically arranged under user-defined groups. When you map a permission to a selected group, the system takes that group into account when determining user permissions.

Adding a custom role

Procedure

1. On the menu bar, click **Administration** > **Roles**.
2. On the **Roles** page, select an existing role, and perform one of the following steps:
   - Click **New**
   - Right-click and select **New**

   The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.
3. On the Add New Role page, fill in the **Role Name** and **Role Description** fields.
4. Click **Commit and Continue**.

   The system displays the Role Details page.

5. On the **Element/Service Permissions** tab, click **Add mapping** to define permissions for a role.

   Alternatively, click **Copy All From** to copy all the permissions on all types of elements or services from an existing role. For instructions, see Copying permission mapping for a role on page 31.

6. Perform one of the following:

   - Option one:

     - Select a group from the **Group Name** field.

       Note:

       Ensure that you create a group before you select the group.

     - (Optional) Select an element or resource type from the **Element or Resource Type** field.

   - Option two:

     - Leave the **Group Name** field blank, and select an element from the **Element or Resource Type** field.

       Based on the element type that you select, the system displays the available elements in the **Element or Resource Instance** field.

     - In the **Element or Resource Instance** field, select an individual element or select `All`.

7. Click **Next**.

   The title of the Permission Mapping page displays the element type that you selected.

8. On the Permission Mapping page, modify the permissions that are available for this role as appropriate.

   The system displays permissions that are available for the parent of the role that you created. The system displays the permissions that are not assigned to the parent role as read-only. As an administrator, you can deny, modify, or view the permissions associated with a role.

9. Click **Commit**.

   The system displays the Role Details page with the permissions that you selected.

10. Click **Commit** to confirm your settings.

Add New Role field descriptions

Field	Description
Role Name	The name of the custom role that you require to add. The name must be between 1 to 256 characters in length. Allowed characters include a-z, A-Z, 0-9, and, _. You can add up to 1500 roles.
Role Description	A brief description of the role that you add.

Button	Description
Commit and Continue	Saves the role name and description and takes you to the Roles Details page.
Cancel	Cancels the permission mapping and takes you back to the Roles page.

Mapping permissions using the template

About this task

Use this procedure to edit or map permissions of the selected element using the template.

Procedure

1. On the menu bar, click **Administration** > **Roles**.
2. On the Roles page, select a role and click **Edit**.
3. On the **Element/Service Permissions** tab, click **Add Mapping**.
4. On the **Element or Resource Type** field, select an element from the drop-down list.
5. On the **Element or Resource Instance** field, select an instance.
6. Click **Next**.

   The system displays the permission mapping for the element you selected.
7. Perform the following as appropriate to modify the permissions:
   - Select a different permission from the **Template for permission set** field.
   - Or, select or clear the permissions to edit the existing permissions for the element.
8. Click **Commit**.

Add mapping field descriptions

Field	Description
Group Name	The name of the group that you must select for the role. The options are: • Select a group. The **Element or Resource type** field is optional. • Leave the field blank. The **Element or Resource type** becomes mandatory.
Element or Resource type	Element types that are available. The options are: • The field is optional if you have selected a group in the **Group Name** field. • Select an element type. The system displays elements in the **Element or Resource Instance** field based on the element type that you select in this field.

Table continues…

Field	Description
Element or Resource Instance	The elements that are available or resource instance. Based on the element type that you selected in **Element or Resource type** field, this field lists the available elements.

Button	Description
Next	Saves your changes in this page and takes you to the Permission Mapping page.
Cancel	Cancels your selection and takes you to the Roles Details page.

Assigning users to a role

Procedure

1. On the menu bar, click **Administration** > **Roles**.
2. On the Roles page, select a role and click **Edit**.
3. On the Role Details page, click the **Assigned Users** tab.
4. Click **Select Users** to assign a role to individual users or edit a role.

   The system displays the Assigned Users page.

   Note:

   The system does not display the end users in the **Assigned Users** list.
5. Select users to whom you must assign the role.
6. Click **Commit**.

   The system displays the permissions for the role on the Role Details page.

Assigned users field descriptions

The system displays the Assigned Users page when you click **Select Users** on the **Assigned Users** tab of the Role Details page. You can select users to grant permissions associated with this role.

Name	Description
User Name	The name of the user you assign to the role.
Full Name	The full name of the user who is assigned to the role.
Type	The type of user: • Local- Users stored in the directory server of AFO. • External- Users stored in the directory server of the customer.

Button	Description
Commit	Assigns the users that you select to the role.
Cancel	Cancels your action and takes you to the Role Details page.

Unassigning users from role

Procedure

1. On the menu bar, click **Administration** > **Roles**.
2. On the Roles page, select a role and click **Edit**.
3. On the Role Details page, click the **Assigned Users** tab.
4. Click **Selected Users**.
5. On the Assigned Users page, clear the check box of the user that you must unassign.
6. Click **Commit**.

Copying permission mapping for a role

Procedure

1. On the menu bar, click **Administration** > **Roles**.
2. On the Roles page, select a role and click **Edit**.
3. On the Role Details page, click the **Assigned Users** tab.
4. Click **Copy All From**.

   The system displays the Permission Mapping page.
5. Select a role from the **Copy From Role** field.

   The system displays all child roles of the parent of this role and all child roles of this role.

   Note:

   Using the **Copy From Role** option, you cannot copy permissions from the Network Administrator and System Administrator roles.
6. Click **Copy**.

   The system displays the Role Details page.
7. Click **Commit**.

   The system displays the Roles page where you can view the details of the role.

Editing a custom role

Procedure

1. On the menu bar, click **Administration** > **Roles**.
2. On the Roles page, select a role and click **Edit**.

3. On the Role Details page, modify the **Role Name** and **Description** fields.
4. Click **Commit and Continue**.
5. On the **Element/Service Permissions** tab, Click **Add Mapping** and modify the permissions for a role as appropriate.

   For information, see Mapping permissions using the template on page 29.
6. Click **Commit**.

Role Details field descriptions

Field	Description
Role Name	The name of the custom role that you require to add. The name must be between 1 to 256 characters in length. Allowed characters include a-z, A-Z, 0-9, and, _.
Role Description	A brief description of the role that you add.

Button	Description
Commit	Saves the changes takes you to the Roles page.
Cancel	Cancels the permission mapping and takes you back to the Roles page.
Add Mapping	Displays the permissions page where you can map permissions for the role.
Delete Mapping	Allows you to delete an existing permissions set.
Copy All From	Displays the Permission Mapping page where you can copy an existing permission set.

Deleting the custom roles

Procedure

1. On the menu bar, click **Administration** > **Roles**.
2. On the Roles page, select one or more roles that you must delete and perform one of the following steps:
   - Click **Delete**
   - Right-click and select **Delete**
3. On the Delete Roles page, click **Delete** to proceed with the deletion.

   When you delete a role, the system deletes all child roles of the role.

   You cannot delete the implicit roles from the Roles page. However, the system deletes the implicit roles when the administrator deletes the tenant.

Roles field descriptions

The Roles page contains two panes. The left pane displays the tree structure of roles. The right pane displays the details of the role that you select on the left pane.

Field	Description
Role Description	A brief description of the role.
No of users	Number of users associated with the role.
Elements	Name of the element mapped to the role.

Button	Description
New	Displays the Add New Role page where you can add a custom role.
Delete	Displays the Delete Roles page where you can confirm the deletion of the custom role.
Edit	Displays the Role Details page where you can modify the custom role.
🔍	Searches for the role based on the search text.
⌫	Clears the search text.

User Administration

This section provides information about managing users. The administrator can perform the user management tasks required to manage users within the AFO.

Viewing existing users

About this task

Perform this procedure to view the users who are configured for AFO access.

Before you begin

Ensure that you are logged on to the AFO as an administrator.

Procedure

1. On the menu bar, click **Administration** > **Users**.

   The Administrative Users page displays.

   The Administrative Users page lists users configured for access to AFO.

2. View the information for existing users.

Adding a new local or external user

About this task

Perform this procedure to create a new user of AFO and to assign roles to the new user.

Before you begin

Ensure that you are logged on to the AFO as an administrator.

Procedure

1. On the menu bar, click **Administration** > **Users**.

   The system displays the Administrative Users page.

2. Click **Add**.

   The system displays the Add New Administrative User page.

3. On the **User ID** field, enter the user ID.

4. On the **Authentication Type** option, select the user type.

   - Local
   - External

5. On the **Full Name** field, enter the full name of the user.

6. On the **Temporary password** field, enter the temporary password.

   Important:

   The password that you enter for the new local user is temporary. After the new user logs on to the AFO for the first time, they are required to change this password. Therefore, Avaya recommends that users record the new password in a secure place.

7. On the **Re-enter password** field, re-enter the temporary password, and then click **Commit and Continue**.

   The Add New Administrative User Step 2 page displays.

8. On the **Role Name** column, select the Role Name check boxes that you want to assign to the user, and then click **Commit**.

   The new user displays in the users list.

Add a new local / external user field description

Field	Description
User ID	ID of the user. This field can accept (1-31) characters and allows characters, a-z, A-Z, 0-9, ., @, - and _.

Table continues…

Field	Description
Authentication type	Type of user: Local user or External user.
Full Name	Full name of the user.
Temporary password	New password for the user. This field allows characters such as lowercase letters (a-z), uppercase letters (A-Z), numbers (0-9) and special characters ({}|()<>,/.=[]_@!$%-+":?`\;). The minimum length of the password is 8 characters.
Re-enter password	Reenter the new password for the user.
Role Name	Roles that a new user can perform.

Disabling a user

About this task

Perform this procedure to disable a user in the AFO network.

Before you begin

- Ensure that you are logged on to the AFO as an administrator.

Procedure

1. On the menu bar, click **Administration** > **Users**.
2. On the Administrative Users page, under **User ID**, select the User ID check box that you want to disable, and then click **Disable**.

   The Account Status for the selected user changes to Disabled.

Deleting a user

About this task

Perform this procedure to delete a user in the AFO network.

Before you begin

- Ensure that you are logged on to the AFO as an administrator.

Procedure

1. On the menu bar, click **Administration** > **Users**.
2. Under **User ID**, select the User ID check box that you want to delete, and then click **Delete**.

   The Delete Users page displays.
3. After you are prompted to confirm the deletion of user, click **Delete**.

Important:

Users cannot delete their own account.

Configuring user properties

About this task

Perform this procedure to change the password and full name for a user, to disable and enable a user account.

Before you begin

- Ensure that you are logged on to the AFO as an administrator.

Procedure

1. On the AFO menu bar, click **Administration** > **Users**.

   The system displays the Administrative Users page.
2. Under **User ID**, click the User ID to which you want to set properties and assign roles.

   The User Details (*User ID*) page displays.
3. To disable or enable the user, select the disabled or enabled option button.
4. On the **Password Reset** section, in the **Password** field, enter a new password.
5. On the **Re-enter password** field, type the new password again.
6. **(Optional)** In the **Full Name** field, edit the name of the user.
7. Click **Commit**.

User Properties field descriptions

Field		Description
User status	Enabled	Enables the user ID.
	Disabled	Disables the user ID.
Password		New password of the user. This field allows characters such as lowercase letters (a-z), uppercase letters (A-Z), numbers (0-9), and special characters ({}|()<>,/.=[_@]!$%-+":?`\;). The minimum length of the password is 8 characters.
Re-enter password		Reenter the new password for the user.
Full Name		Full name of the user.
Authentication type	Local	The user is authenticated by the default Open LDAP service.

Table continues…

Field		Description
	External	The user is authenticated by the external authentication service if it is configured. The External Identity Repositories Web page contains a summary page for authentication scheme and authentication servers. In the Authentication Servers page you can optionally configure an external LDAP server, Radius server, or a 9 Kerberos server.
User ID		ID of the user. This field can accept (1-31) characters and allows characters, a-z, A-Z, 0-9, ., @, - and _.

Editing user role mapping

Before you begin

- Ensure that you are logged on to the AFO as an administrator.

About this task

Perform this procedure to select roles to authorize a user for associated features and element permissions.

Procedure

1. On the AFOmenu bar, click **Administration** > **Users**.

   The system displays the Administrative Users page.

2. Under **User ID**, click the User ID to which you want to set properties and assign roles.

   The Users Details (*User ID*) page displays.

3. On the **Roles** section, click **Select Roles**.

   The system displays the User Roles page for the selected user.

4. On the **Roles** section, select or deselect the **Role Name** check box, and then click **Commit**.

   The system displays the User Details page.

5. Click **Commit**.

External authentication scheme and authentication server configuration

This section provides information about configuring external authentication scheme and authentication server for AFO.

The AFO supports up to four authentication authorities:

- local servers
- external RADIUS servers
- external LDAP servers, including Sun ONE or Microsoft active directory server
- KERBEROS servers

The authentication server policy controls the settings for the external SAML, LDAP, RADIUS, and KERBEROS servers.

Editing the authentication scheme

About this task

Perform this procedure to edit the authentication scheme.

Before you begin

Ensure that you are logged on to the AFO as an administrator.

Procedure

1. On the AFO menu bar, click **Administration** > **System Management**.

   The system launch the SMGR page in a separate browser.

2. On the SMGR page, click **Administrators** > **External Authentication**.

   The system displays the External Identity Repositories page.

3. On the **Authentication Scheme** section, click **Edit**.

   The system displays the Authentication Scheme page.

4. Select the required authentication scheme, and then click **Save**.

Configuring authentication servers

Perform this procedure to configure authentication servers.

When the target LDAP server is not the Microsoft Active Directory, the external user must have the UID attribute mapped to their logon name. When the LDAP server is the Microsoft Active Directory, the full name of the external user must be the same as the logon name that makes the CN attribute of the external users the same as the login name.

The TCP port that is used for the external LDAP server and the UDP port used for the external RADIUS server must be open in the Linux iptables firewall on both the primary security service and backup primary security service. To check the status of the iptables rules, use service iptables status.

In the Authentication Servers page, the administrator has the option of provisioning a LDAP, RADIUS, or KERBEROS server.

Provisioning the LDAP server

About this task

Perform this procedure to complete the required information for the first and second LDAP authentication server.

Note:

Perform same procedure as below to configure **Provision Second LDAP Server**.

Before you begin

- Ensure that you are logged on to the AFO as an administrator.
- Ensure the Linux iptable firewall setting on both the primary and backup security service allows the TCP port as source port.

Procedure

1. On the AFO menu bar, click **Administration** > **System Management**.

   The system launch the SMGR page in a separate browser.

2. On the SMGR page, click **Administrators** > **External Authentication**.

   The system displays the External Identity Repositories page.

3. On **Authentication Servers** section, click **Configure**.

   The Authentication Servers page displays.

4. Select the **Provision First LDAP Server** check box, and complete the following information in the Provision First LDAP Server section:

   - **IP (or DNS)** : Enter the IP address or DNS name of the LDAP server.
   - **TCP Port** : Enter the TC port number of the LDAP server.
   - **Base Distinguished Name**: Enter the base DN of the LDAP server.
   - **SSL/TLS Mode**: Select the check box if the LDAP server supports SSL/TLS connections.
   - **Is Active Directory** : Select the check box if the active directory does not support anonymous binding.
   - **Distinguished Name for Root Binding**: Enter the distinguished name for the root binding.
   - **Password for Root Binding** : Enter the password for the root binding.

5. Click **Save**.

Provisioning the RADIUS server

About this task

Perform this procedure to complete the required information for the RADIUS authentication server.

Before you begin

- Ensure that you are logged on to the AFO as an administrator.

- Ensure the Linux iptable firewall setting on both the primary and backup security service allows the UDP port as source port.

Procedure

1. On the AFO menu bar, click **Administration** > **System Management**.

   The system launch the SMGR page in a separate browser.
2. On the SMGR page, click **Administrators** > **External Authentication**.

   The system displays the External Identity Repositories page.
3. On the **Authentication Servers** section, click **Configure**.

   The Authentication Servers page displays.
4. Select the **Provision Radius Server** check box, and complete the following information in the Provision RADIUS Server section:

   - **IP (or DNS):**: Type the IP address or DNS name of the primary RADIUS server.
   - **UDP Port:** : Type the UDP port number of the primary RADIUS server.
   - **Shared Secret** : Type the shared secret of the RADIUS server.

   Note:

   You must create two records in the external RADIUS server with the same shared secret for both the primary security server and backup security server IP address.

Provisioning the Kerberos server

About this task

To use Kerberos authentication, configure AFO with the required information for the Kerberos server.

Before you begin

- If you use Firefox to gain access to AFO, perform the following:
  1. Type `about:config` in the address bar of the Web browser.
  2. Select the network.negotiate-auth.trusted-uris attribute.
  3. Right-click, select **Modify**, and add the URL of AFO.
- Log on to AFO as admin.

Procedure

1. On the AFO menu bar, click **Administration** > **System Management**.

   The system launch the SMGR page in a separate browser.
2. On the SMGR page, click **Administrators** > **External Authentication**.

   The system displays the External Identity Repositories page.
3. On the **Authentication Servers** section, click **Configure**.

   The system displays the Authentication Servers page.

4. Select the **Provision Kerberos Server** check box, and complete the following information in the Provision Kerberos Server section:
    - **DC Host Name (FQDN)**: Enter your FQDN in the format `machineName.domainName.com/net/`.
    - **DC Computer Domain**: Enter the domain name of the Kerberos server.
    - **Keytab File**: Click **Browse** and select the Kerberos server key file.
5. Click **Save**.

    Important:

    When you log on to the Kerberos server using Single Sign-on (SSO) , the system automatically authenticates you inside the Domain Controller (DC) domain. Therefore, you cannot exit from AFO using the Logout link. Close the Web browser to exit the application.

Provisioning SAML Remote Identity Provider

About this task

Perform this procedure to complete the required information for the SAML Remote Identity Provider.

Procedure

1. On the AFO menu bar, click **Administration** > **System Management**.

    The system launch the SMGR page in a separate browser.
2. On the SMGR page, click **Administrators** > **External Authentication**.

    The system displays the External Identity Repositories page.
3. On the **Authentication Servers** section, click **Configure**.

    The system displays the Authentication Servers page.
4. Select the **Provision SAML Remote Identity Provider** check box, and complete the following information in the Provision SAML Remote Identity Provider section:
    - **Metadata Type**: Specify the method to query the metadata for Remote Identity Provider.
    - **Metadata Url**: Enter the valid HTTP URL.
    - **Metadata File**: Click **Browse** and select the metadata file.
5. Click **Save**.

Provisioning User Certificate Authentication

About this task

Perform this procedure to assign the user certificate authentication

Procedure

1. On the AFO menu bar, click **Administration** > **System Management**.

    The system launch the SMGR page in a separate browser.

2. On the SMGR page, click **Administrators** > **External Authentication**.

   The system displays the External Identity Repositories page.
3. On the **Authentication Servers** section, click **Configure**.

   The system displays the Authentication Servers page.
4. On the **User Certificate Access Level**, select the user certificate access level from the list.
5. Click **Save**.

Authentication Servers field descriptions

Provision LDAP Server

Name	Description
IP (or DNS)	Specifies the IP address or the DNS name of the LDAP server.
TCP Port	Specifies the TCP port of the LDAP server.
Base Distinguished Name	Specifies the base distinguished name of the LDAP server.
SSL/TLS Mode	Specifies whether the LDAP server supports SSL/TLS connections.
Is Active Directory	Select this check box if active directory does not support anonymous binding.
Distinguished Name for Root Binding	Type the distinguished name for the root binding. For example, type cn for Users.
Password for Root Binding	Type the password for the root binding in this field.

Provision Radius Server

Name	Description
IP (or DNS)	Specifies the IP address or the DNS name of the primary RADIUS server.
UDP Port	Specifies the UDP port number of the primary RADIUS server.
Shared Secret	Shared secret of the RADIUS server.

Provision Kerberos Server

Name	Description
DC Host Name (FQDN)	Enter your FQDN in the following format: `machineName.domainName.com/net/`.
DC Computer Domain	Specifies the domain name of the Kerberos server.
Keytab File	Type the encrypted Kerberos server key in this field.

Provision SAML Remote Identity Provider

Name	Description
Metadata Type	Specifies the method to query the metadata for Remote Identity Provider. The values are: • URL: A valid HTTP URL. • File: A valid XML file
Metadata Url	Specifies the valid HTTP URL for the metadata of Remote Identity Provider.
Metadata File	Specifies the valid XML file for the metadata of Remote Identity Provider or click **Browse** to select an XML file that contains the metadata for Remote Identity Provider.

Configuring SAML

The system automatically configures AFO as Hosted Service Provider during the installation or upgrade of AFO. However, you can customize configuration on the Hosted Service Provider for external SAML authentication and on the Hosted Identity Provider for SAML authentication in the domain.You can modify the configuration using the following procedure.

As an administrator, you can enable or disable SAML authentication in AFO from the **System Management** page.

Editing SAML Hosted Service Provider properties

About this task

Perform this procedure to modify the configuration.

Procedure

1. On the AFO menu bar, click **Administration** > **System Management**.

   The system launch the SMGR page in a separate browser.

2. On the SMGR page, click **Administrators** > **SAML Configuration**.

   The system displays the SAML Configuration page.

3. Click **Edit**.

4. On the **SAML Hosted Service Provider** page, perform the following:

   - Select the **NameID as UserID** check box.
   - On the **Attribute Used as UserID** field, enter the name of the attribute that you want to use as the login ID of the user in AFO.

- On the **Mapped Attributes** field, enter an attribute that you require to map between RIDP and H-SP for a user and click **Add**.

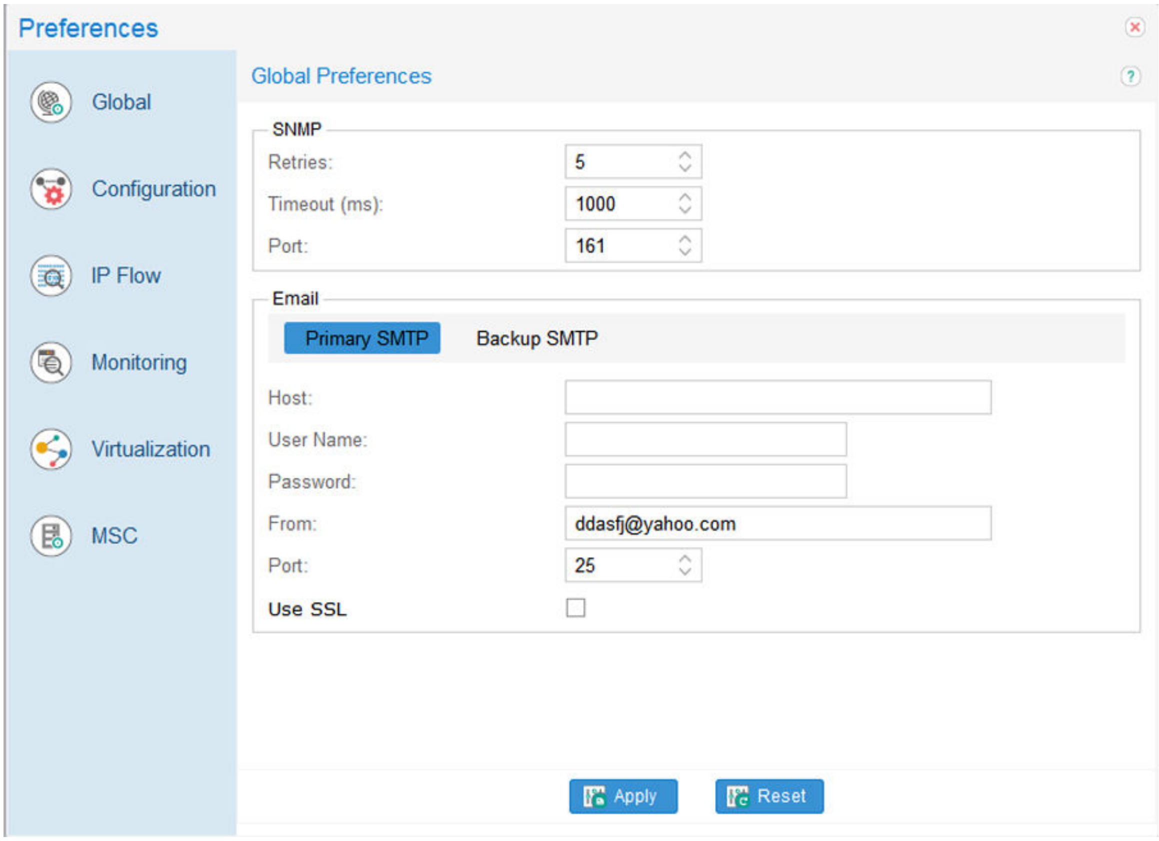
  Select the attribute which you want to remove from the **Mapped Attributes** list and click **Remove**.

5. Click **Save**.

Chapter 7: Managing Preferences

Preference management allows you to define and retain the settings and other properties of the system across multiple sessions.

From the AFO dashboard, click the Preferences icon from the quick access toolbar to open the preferences page. On the Preferences page, the **Preferences** navigation pane is located on the left side of the page.



SNMP

Retries: 5

Timeout (ms): 1000

Port: 161

Email

Host:

User Name:

Password:

From: ddasfj@yahoo.com

Port: 25

Use SSL ☐

Figure 2: Preferences page

The root level items of the Preferences navigation pane are:

- Global
- Configuration
- IP Flow
- Monitoring

- Virtualization
- MSC

Configuring Global Preferences

This section provides information about configuring global preferences in the Avaya Fabric Orchestrator (AFO). Use Global Preferences to manage preferences used by multiple applications across the entire AFO.

Note:

The system displays the Global Preferences tab as the default view on the preferences page.

Global Preferences page displays the SNMP and E-mail preferences on the right side of the page and displays a navigation pane on the left side of the page.

About this task

Use Global Preferences to configure preferences that apply to more than one service.

Perform this procedure to configure the SNMP and E-mail preferences on AFO.

AFO provides SNMP and E-Mail preferences under the Global Preferences to configure these preferences for multiple services simultaneously and to avoid configuring these preferences in multiple locations.

Procedure

1. From the AFO dashboard, click preferences icon from the quick access toolbar to open the **Preferences** page.

   The **Preferences** page displays global preferences as the default view on the right side of the page.
2. In the SNMP section, enter or edit the values for **Retries, Timeout, and Port** fields.
3. In the Email section, click **Primary SMTP**:
   a. Enter or edit the primary SMTP **Host, User Name, Password, From, and Port** fields.
   b. Select or clear the **Use SSL** checkbox.

      Secure Sockets Layer is the standard security technology for establishing an encrypted link between a web server and a browser.
4. **(Optional)** In the Email section, click **Backup SMTP**:
   a. Enter or edit the primary SMTP **Host, User Name, Password, From, and Port** fields.
   b. Select or clear the **Use SSL** checkbox.
5. Click **Apply**.

Next steps

See Global Preferences field descriptions on page 47 for field descriptions and appropriate default values.

Global Preferences field descriptions

Field		Description
SNMP	Retries	Specifies the number of retries to be attempted when a response is not received for a generated message. • Default value: 3 • Maximum Retries: 10
	Timeout (ms)	The number of milliseconds an element polls a device without receiving a response before timing out. • Default value: 1 minute
	Port	Specifies the primary port number of the SNMP server.
Primary SMTP	Host	Specifies the primary host AFO uses to set up a connection to the corporate e-mail server.
	User Name	Specifies the primary SMTP user name (example: john.doe@avaya.com).
	Password	Specifies the primary Password that permits AFO to set up a connection to the corporate e-mail server.
	Port	Specifies the primary port number.
	From	Specifies the sender address to determine who the message is from.
	Use SSL	Specifies the secure socket layer connection. Select the check box for secure connection.
Backup SMTP	Host	Specifies the backup host AFO uses to set up a connection to the corporate e-mail server.

Table continues…

Field		Description
	User Name	Specifies the backup SMTP user name (example: john.doe@avaya.com).
	Password	Specifies the backup Password that permits AFO to set up a connection to the corporate e-mail server.
	From	Specifies the sender address to determine who the message is from.
	Port	Specifies the backup port number.
	Use SSL	Specifies the secure socket layer connection. Select the check box for secure connection.

Configuration Preferences

Configuring Configuration Preferences

Application preferences also manages a set of AFO Configuration server preferences. Use the following procedures to configure general and logging preferences.

From the AFO dashboard, click preferences icon from the quick access toolbar to open the **Preferences** page.

Configuring General System preferences

Perform the following procedure to configure the general system preferences:

Procedure

1. On the **Preferences** page, click **Configuration** from the left navigation pane.

   The Preferences page displays the **Configuration** on the right side of the page.

2. Click the **General** tab.

   The **General** pane displays.

3. In the SNMP section, for the **Max Outstanding Requests [20..250]** list:

   Enter the number of SNMP requests, between 20 and 250, that AFO Configuration maintains as open or outstanding. The default value is 100.

4. In the **Email** section enter field values in the following fields:
   - **From User**: The E-mail address of the sender.
   - **To Recipient**: The E-mail address of the recipient.
   - **Enable Email**: If selected, enables the E-mail function.
5. Click **Test Email** to test the E-mail server.
6. Click **Apply** to save the preferences.

   Note:

   To reset the configuration or to discard the changes, click **Reset**.

Configuring logging information

Perform the following procedure to configure logging.

Logging Audit Log

About this task

Perform the following procedure for logging audit log.

Procedure

1. On the **Preferences** page, click **Configuration** from the left navigation pane.

   The Preferences page displays the **Configuration** on the right side of the page.
2. Click the **Logging** tab.

   The **Logging** pane displays.
3. In the Audit Log section, enter appropriate values in the following fields:
   - **File Size**: Enter the audit log file size. The default value is 10 MB.
   - **Log Level**: Select the audit log level from the list. The default value is `INFO`.
   - **No. Of Files [1–10]**: Select the number of files that are archived. The default value is 3.
   - **Purge logs older than**: Select the retention limit for the audit logs by selecting the number of weeks or months in the combo boxes. The default value is 6 months.
   - Archiving Audit Logs:

     Archive logs before purging to: Select the check box to save the audit log backup files in CSV format.

     The audit logs are automatically saved to the following location: `/opt/avaya/smgr/com/log/Audit_Archives`.
   - Deleting audit logs

     Delete Permanently: Select the check box to delete audit log files without creating backup files.
4. Click **Archive**.

A confirmation dialog box appears.

5. Click **Apply**.

Next steps

Perform the procedure for Logging Debug Log on page 50.

Logging Debug Log

About this task

Perform the following procedure for logging debug log.

Before you begin

You must configure the audit log. For more information, see Logging Audit Log on page 49.

Procedure

1. On the **Preferences** page, click **Configuration** from the left navigation pane.

   The Preferences page displays the **Configuration** on the right side of the page.

2. Click the **Logging** tab.

   The **Logging** pane displays.

3. In the Debug Log section, enter appropriate values in the following fields:

   - **File Size**: Enter the Debug Log file size. The default value is 10 MB.
   - **Log Level**: Select the Debug Log level from the list. The default value is `ALL`.
   - **Trace**: Select the check box to add additional SNMP information in the error log, and this can provide assistance while troubleshooting.

     Important:

     Selecting Trace can slightly slow down performance as extra information is gathered.

   - **No. Of Files [1–10]**: Select the number of files that are debugged. The default value is 3.

4. Click **Apply** to save the preferences.

   Note:

   To reset the configuration or to discard the changes, click **Reset**.

Configuring IP Flow management preferences

Use the following procedures to manage preferences and configure parameters for AFO IP Flow administration and top 10 tools.

- Configuring collector information on page 51
- Configuring the capture duration and look back time on page 52

- Configuring Monitoring Server Configuration on page 53
- Starting and stopping IPFIX Collector on page 53

From the AFO dashboard, click preferences icon from the quick access toolbar to open the **Preferences** page.

Configuring collector information

Use this procedure to provide the AFO IP Flow server with the following information:

- UDP ports for collecting data — AFO IP Flow uses UDP Ports to receive IP flow data from devices. To increase the load of the server as well as to improve performance after multiple IPFix devices are enabled, specify two UDP ports to receive IP flow data instead of one. Configure half the devices to send flow information to Port 1 and the other half to Port 2.
- Option for data analysis — AFO IP Flow uses **Show DNS Name** and **Show IP Address** for data analysis. Select **Show DNS Name** to display the domain name assigned to each of the participating device in the network or **Show IP Address** to display the IP Address of the device in the network.
- Notification E-mail address — AFO IP Flow uses an E-mail address to send a message to after the number of flows exceeds the maximum license limit.

Procedure

1. On the **Preferences** page, click **IP Flow** from the left navigation pane.

   The Preferences page displays the **IP Flow** on the right side of the page.
2. In the UDP Port 1 field, enter a UDP port for collecting data.
3. In the UDP Port 2 field, enter a second UDP port for collecting data.
4. In the Data Analysis Option field, select an option for data analysis.

Choice Option	Choice Description
Show IP Address	Displays an Internet Protocol address (IP address) assigned to each of the participating devices in the network.
Show DNS Name	Displays the domain assigned to each of the participating devices in the network.

5. In the Notification Email field, enter an E-mail address to which AFO IP Flow sends a collector E-mail notification when IPFIX data exceeds the license limit.

Next steps

Perform the procedure for Configuring the capture duration on page 52.

Variable definitions

Table 4: Variable definitions for configuring collector information

Variable	Value
UDP Port 1	Enter a UDP port for collecting data.
UDP Port 2	Enter a second UDP port for collecting data.
Data Analysis Option	Select an option for data analysis. The options are: • Show DNS Name • Show IP Address
Notification Email	Enter an E-mail address to which the system sends a collector E-mail notification when IPFIX data exceeds the license limit.

Configuring the capture duration and look back time

Use this procedure to configure the following information.

- Time (min) — Configure capture duration time greater than one minute.
- Look back time (minutes/hours) — Configure a look back time interval for the Top 10 Views.

Before you begin

You must configure the following Flow preference:

- Collector Configuration — For more information, see Configuring collector information on page 51.

Procedure

1. On the **Preferences** page, click **IP Flow** from the left navigation pane.

   The Preferences page displays the **IP Flow** on the right side of the page.

2. In the Time (min) field, select a capture duration time in minutes.

Choice Option	Choice Description
Minutes	Select a capture duration value between 1 and 5 minutes.

3. In the Look back time (minutes/hours) field, for minutes enter a value between 1 and 4,320. For hours, enter a value between 1h and 72h

Choice Option	Choice Description
Minutes	Enter a positive value between 1 and 4.320 as a look back interval for the Top 10 Views.
Hours	Enter a positive value between 1h and 72h as a look back interval for the Top 10 Views.

Next steps

Perform the procedure for Configuring Monitoring Server Configuration on page 53.

Configuring Monitoring Server Configuration

Before you begin

You must configure the following IP Flow preferences:

- Collector configuration — For more information, see Configuring collector information on page 51.
- Capture duration — For more information, see Configuring the capture duration and Look back time on page 52.

Procedure

1. On the **Preferences** page, click **IP Flow** from the left navigation pane.

   The Preferences page displays the **IP Flow** on the right side of the page.

2. In the Monitoring Server Configuration section:

   Domain (read-only) field, displays `AFO` as the discovered domain from the monitoring server.

3. Click **Apply**.

Starting and stopping IPFIX Collector

The status of the IPFIX Collector is visible in the Collector section. Use this procedure to start or stop IPFIX Collector. You can restart the IPFIX Collector when the status is in Running mode only.

IPFIX Collector is a standalone process that collects IPFIX packets received from configured devices. Use this tool to monitor, view, and diagnose problems and resource consumption at the application level in a multi-vendor network environment.

The IPFIX Collector is in the started state by default. You can stop and restart the Collector in case of configuration changes to IP Flow as well as for troubleshooting issues.

You can configure IP Flow Preferences in any state but you must restart the IPFIX Collector after configuring the preferences.

Procedure

1. On the **Preferences** page, click **IP Flow** from the left navigation pane.

   The Preferences page displays the **IP Flow** on the right side of the page.

2. In the Collector section, click one of the following icons:

   - To start the IPFIX Collector, click **Start**.
   - To stop the IPFIX Collector, click **Stop**.
   - To restart the IPFIX Collector, click **Re-Start**. You can restart the IPFIX Collector only when the status is in Running mode.

Monitoring Preferences

Configuring Monitoring Preferences

Use the following procedure to manage preferences and configure parameters for traps viewer and syslog viewer. The Traps and Syslogs page enables you to view information for SNMP traps and syslogs reports.

From the AFO dashboard, click preferences icon from the quick access toolbar to open the **Preferences** page.

Configuring Syslog settings

You can configure how syslog information is organized and displayed. Use the following procedure to configure the Syslog Viewer.

You can also configure the syslog settings through the Settings icon on the Syslogs page.

Procedure

1. From the quick access toolbar on the top right, select **Preferences**.
2. Click **Monitoring** from the left hand navigation pane.

   The Monitoring preference page is displayed.
3. On the Monitoring Preferences page, perform the following tasks in the Syslog Configuration section:
   - Set the **Maximum age**. Entries that are older than the maximum age defined in this field are purged from the AFO Monitoring database.
   - Enter the **Maximum number**. After the maximum number of entries are in the AFO Monitoring database, the oldest entries are deleted as new entries are added.
   - Set the **Limit to disc. devices** to true or false. This determines whether the trap data is limited to discovered devices.
   - Enter the **Listener port** (default is 162).
   - Enter the **Archive depth**. Older files beyond this number are deleted.
   - In the **Archive directory** field, enter the file path for the directory where you want archive files to be stored.
   - In the **Forwarding** section, click **Add Forwarder** to enter the Host Address, and port number for syslog information.
4. Click **Apply** to save the changes.

Configuring Trap settings

You can configure how trap information is organized and displayed. Use the following procedure to configure the Trap Viewer.

You can also configure the trap settings through the Settings icon on the Traps page.

Procedure

1. From the quick access toolbar on the top right, select **Preferences**.
2. Click **Monitoring** from the left hand navigation pane.

   The Monitoring preference page is displayed.
3. On the Monitoring Preferences page, perform the following tasks in the Trap Configuration section:
   - Set the **Maximum age**. Entries that are older than the maximum age defined in this field are purged from the AFO Monitoring database.
   - Enter the **Maximum number**. After the maximum number of entries are in the AFO Monitoring database, the oldest entries are deleted as new entries are added.
   - Set the **Limit to disc. devices** to true or false. This determines whether the trap data is limited to discovered devices
   - Set the **Limit to auth. devices** to true or false. This determines whether the trap data is limited to authenticated devices.
   - Enter the **Listener port** (default is 162).
   - Enter the **Archive depth**. Older files beyond this number are deleted.
   - In the **Archive directory** field, enter the file path for the directory where you want archive files to be stored.
   - In the **Forwarding** field, click **Add Forwarder** to enter the destination IP address for trap information.
4. Click **Apply** to save the changes.

Virtualization Preferences

Configuring Virtualization Preferences

Use the following procedure to configure and manage AFO Virtualization preferences in General, vCenter, scheduler, and Logging categories.

From the AFO dashboard, click preferences icon from the quick access toolbar to open the **Preferences** page.

Configuring General settings

About this task

You can configure settings for Global Port Dissociation, Monitor Events Purge, and Network View. From the AFO dashboard, click preferences icon from the quick access toolbar to open the **Preferences** page.

Configuring Global Port Dissociation settings

Perform following steps to configure Global Port Dissociation settings.

Procedure

1. On the **Preferences** page, click **Virtualization** from the left navigation pane.

   The Preferences page displays the **Virtualization** on the right side of the page.

2. Click the **General** tab.

3. In the **Global Port to be dissociated from VLAN** section, select or clear the following check boxes:

Choice Option	Choice Description
Edge Device	If the check box is selected, AFO Virtualization dissociates the port from the VLAN for the edge device, which is connected to the ESX/ESXi server. This field is selected by default.
Core Device	If the check box is selected, AFO Virtualization dissociates the port from the VLAN for the core device (BEB), which is connected to the edge device. This field is cleared by default. **Note:** The **Core Device** field is enabled only if **Edge Device** field is enabled. It is not possible to dissociate ports from the core device alone.

4. Click **Apply**.

Configuring Monitor Event Purge settings

About this task

Perform the following steps to configure Monitor Events Purge settings.

Procedure

1. On the **Preferences** page, click **Virtualization** from the left navigation pane.

   The Preferences page displays the **Virtualization** on the right side of the page.

2. Click the **General** tab.

3. In the Monitor Events Purge section, select or clear the **Enable Monitor Purge** field.

   If the field is selected, Monitor Events Purge is enabled. If the field is not selected, Monitor Events Purge is disabled.

Note:

Monitor Events Purge is enabled by default when you configure AFO for the first time through Day-1 wizard. Monitor Events Purge is not enabled (and scheduled) by default if you cancel the Day-1 wizard.

4. In the Monitor Events Purge section, perform one of the following actions:
   - In the **Retention Time in Days [30 - 90]** field, specify the number of records in days you want to purge from the Event Monitor. The default value is 90.
   - In the **Number of Rows to Retain [10000 - 50000]** field, specify the number of event monitor rows you want to purge. The default value is 50000.

   The purge criteria are independent. When purge is executed based on *Number of Days*, the preference value for *Number of Rows* is ignored. Similarly, when purge is executed on *Number of Rows*, the preference value for *Number of Days* is not taken into account.
5. **(Optional)** In the Monitor Events Purge section, click **Purge Now** to purge all the event monitor records. This action is not dependent on values entered in Retention Time in Days [30 - 90] or Number of Rows to Retain [10000 - 50000].
6. Click **Apply**.

Next steps

- You can view the Monitor Events Purge details in the AFO Virtualization Audit Log. The Audit Log contains an entry for each record, which is purged based on the Number of Days and Number of Rows. For more information, see *Virtualization Configuration using Avaya Fabric Orchestrator*, NN48100–503.

Configuring Network View Setting

About this task

Perform the following steps to configure Network View Settings.

Procedure

1. On the **Preferences** page, click **Virtualization** from the left navigation pane.

   The Preferences page displays the **Virtualization** on the right side of the page.
2. Click the **General** tab.
3. In the View section, select **Network** or **Inventory** from the drop-down list.

   Note:

   By default, topology view is displayed in Network and inventory view is displayed in Inventory.
4. In the View section, select or clear the following check boxes:

Choice Option	Choice Description
Show Device IP	Displays device Internet Protocol (IP address).
Show Device Name	Displays device name.

5. Click **Apply**.

Configuring vCenter Server settings

About this task

Perform the following steps to configure AFO Virtualization preferences related to vCenter access details. From the AFO dashboard, click preferences icon from the quick toolbar to open the **Preferences** page.

Procedure

1. On the **Preferences** page, click **Virtualization** from the left navigation pane.

   The Preferences page displays the **Virtualization** on the right side of the page.
2. Click the **vCenter Server** tab.

   The vCenter Server pane is displayed.
3. In the Primary VCenter Server Information section:
   a. Enter the Hostname or IP Address in the **Hostname/IP Address** field.
   b. Enter the username in the **Username** field.
   c. Enter the password in the **Password** field.
4. In the Primary VCenter Server Information section, to test the connectivity of AFO Virtualization to the vCenter host, click **Validate connection**.

   A pop-up window is displayed with the validation message.
5. Click **Apply**.

Configuring Scheduler settings

You can configure settings for Hypervisor Connectivity, Monitor Purge, and Audit Log Purge jobs. From the AFO dashboard, click preferences icon from the quick access toolbar to open the **Preferences** page.

Rescheduling Hypervisor Connectivity jobs

About this task

Perform the following steps to reschedule Hypervisor Connectivity jobs.

✱ **Note:**

Each time the AFO Virtualization application starts and the AFO Virtualization Discovery Wizard completes, Hypervisor Connectivity is scheduled to run every 24 hours.

Procedure

1. On the **Preferences** page, click **Virtualization** from the left navigation pane.

   The Preferences page displays the **Virtualization** on the right side of the page.
2. Click the **Scheduler** tab.
3. In the Hypervisor Connectivity section, click **Reschedule**.

The Schedule Details window is displayed.

4. In the Schedule Details window, configure the following fields:

Choice Option	Choice Description
Every Month On	Select and enter date from the list to perform operation on a monthly basis.
Every Week On	Select and enter day of the week from the list to perform operation on a weekly basis.
Every Days	Select and enter day from the list, followed by selecting **Date** and **Time**, to perform a operation.
Every Hrs	Select and enter time in hours from the list, followed by selecting **Date** and **Time**, to perform operation on an hourly basis.

5. Click **Save**.

   Save initiates an immediate purge, with the next purge occurring according to the specified interval.

Rescheduling Monitor Purge jobs

About this task

Perform the following steps to reschedule Monitor Purge jobs.

Note:

During the AFO Virtualization installation, when you go through the Day-1 wizard, Monitor Purge is enabled by default and is scheduled to run every 90 days. If you cancel the Day-1 wizard, Monitor Purge is not enabled or scheduled.

Procedure

1. On the **Preferences** page, click **Virtualization** from the left navigation pane.

   The Preferences page displays the **Virtualization** on the right side of the page.

2. Click the **Scheduler** tab.
3. In the Monitor Purge section, click **Reschedule**.

   The Schedule Details window displays.

4. In the Schedule Details window, select the interval as required.
5. Click **Save**.

   Save initiates an immediate purge, with the next purge occurring according to the specified interval.

Rescheduling Audit Log Purge jobs

About this task

Perform the following steps to reschedule Audit Log Purge jobs.

Procedure

1. On the **Preferences** page, click **Virtualization** from the left navigation pane.

The Preferences page displays the **Virtualization** on the right side of the page.

2. Click the **Scheduler** tab.
3. In the Audit Logs Purge section, click **Reschedule**.

   The Schedule Details window is displayed.
4. In the Schedule Details window, select the interval as required.
5. Click **Save**.

   Save initiates an immediate purge, with the next purge occurring according to the specified interval.

Configuring Logging settings

You can configure settings for Audit Log Configuration and Debug Log Configuration. From the AFO menu bar, click preferences icon from the quick access toolbar to open the **Preferences** page.

Configuring Audit Log

About this task

Perform the following steps to configure Audit Log settings.

Procedure

1. On the **Preferences** page, click **Virtualization** from the left navigation pane.

   The Preferences page displays the **Virtualization** on the right side of the page.
2. Click the **Logging** tab.

   The Logging pane is displayed.
3. In the Audit Log Configuration section, configure the following settings:
   - In **Level** field, select **On** or **Off** from the drop-down list.
   - Select or clear **Enable Purge** check box, to enable or disable purge.
   - In **Retention Time in Days [15–120]** field, specify the number of records in days you want to purge. The default value is 60.
4. Click **Apply**.

Configuring Debug Log

About this task

Perform the following steps to configure Debug Log settings.

Procedure

1. On the **Preferences** page, click **Virtualization** from the left navigation pane.

   The Preferences page displays the **Virtualization** on the right side of the page.
2. Click the **Logging** tab.

   The Logging pane is displayed.

3. In the Debug Log Configuration section, configure the following settings:
    - In **File Size** field, enter the maximum file size. The default value is 10 MB.
    - In **Level** field, select **Off**, **Error**, **Warn**, **Info**, or **Debug** log level from the list.

      The default is `Info`.
    - In **No. of Files [1–10]** configure the number of log files. The default value is 3.
4. Click **Apply**.

Configuring MSC Preferences

About MSC Preferences

Use MSC preferences to configure preferences related to Management Server Console, PLDS, and Software Library. This section provides information about launching and configuring Management Server Console (MSC) preferences in the Avaya Fabric Orchestrator (AFO).

Scenario 1: AFO Dashboard

1. From the AFO menu bar, click the Preferences icon from the quick access toolbar to open the **Preferences** page.
2. On the **Preferences** page, click **MSC** from the left navigation pane to open the MSC Preferences pane.

   The **Preferences** page displays the **MSC** preference pane on the right side of the page.

Scenario 2: Solution Software Director (SSD)

You can launch MSC preferences from the SSD page when platform service is down.

1. Login to SSD through the MSC server URL `https://<Fully Qualified Domain Name of MSC Server>/SSD`.
2. Enter system user name and password to access the platform.
3. On the AFO menu bar, click **Administration** > **Solution Software Director**. You can launch **MSC** from any one of the given option:

Choice option	Description
Work Flow	• You can launch **MSC Preferences** from the **Work Flow** section on the **Software Director** page. • Click (>) symbol on the top-left corner sidebar of the **Solution Software Director** home page

Table continues…

Choice option	Description
	to open **Work Flow**. Click **Utilities** > **MSC preferences**.
MSC Preferences	• You can launch **MSC Preferences** from the **MSC Preferences** icon on the top toolbar of the **Solution Software Director** home page. • On the **Solution Software Director** home page, click **MSC Preferences** icon from the top toolbar to open **MSC preferences** page.

Configuring PLDS settings

Use the following procedure to configure Product Licensing and Delivery System (PLDS) information using PLDS preferences. You need PLDS information for entitlements and to download license files

Before you begin

- From the AFO dashboard, click preferences icon from the quick access toolbar to open the **Preferences** page.

  Note:

  When the platform service is down, open **Preferences** page from Solution Software Director (SSD) page. See About MSC Preferences on page 61 for more information.

Procedure

1. On the **Preferences** page, click **MSC** from the left navigation pane to open the MSC preference page.

   The system displays the **MSC** preference page with **PLDS** as default tab.

2. On the **PLDS** section:
   - Enter the user ID in the **User ID** field.
   - Enter the PLDS password in the **Password** field.
   - Enter the sold to ID in the **Sold to ID** field.

3. Select the **Use Proxy** check box and enter the proxy IP address in **Proxy IP** field, to configure the proxy server details.

4. Click **Apply** to save.

Configuring Integrated Lights-Out settings

Use the following procedure to configure HP Integrated Lights-Out (iLO); IP Address and SNMP Settings (v1 and V3) as part of configuration of the AFO Appliance.

Note:

If any settings are changed directly on iLO, MSC will overwrite these settings so that there is no ambiguity.

Before you begin

- From the AFO menu bar, click preferences icon from the quick access toolbar to open the **Preferences** page.

  Note:

  When the platform service is down, open **Preferences** page from Solution Software Director (SSD) page. See About MSC Preferences on page 61 for more information.

Procedure

1. On the **Preferences** page, click **MSC** from the left navigation pane to open the MSC preference page.

   The **MSC** preference page is displayed with **PLDS** as default tab.
2. Click the **iLO** tab.

   The system displays the **iLO** page.
3. On the **SNMP v3** section enter the user name, authentication password, and privacy password in their respective fields.
4. Click **Apply**.

Configuring External Storage settings

Use this procedure to configure external storage settings on Avaya Fabric Orchestrator (AFO) for backup, upgrade, and logging tasks. You can configure the following three protocols in AFO for transferring files.

- Secure Copy Protocol (SCP)
- File Transfer Protocol (FTP)

Procedure

1. On the **MSC Preferences** page, click **External Storage** tab.

   The system displays the **External Storage** paneMSC Preferences.
2. In the **SCP** section configure Secure Copy Protocol (SCP) for transferring files across secure network.
   - Enter the server IP/FQDN details in the **Server IP/FQDN** field.
   - Enter the root directory in the **Root Directory** field.
   - Enter the user name in the **User name** field.
   - Enter the password in the **Password** field.
3. In the **FTP** section configure File Transfer Protocol (FTP) for transferring files.
   - Enter the server IP/FQDN details in the **Server IP/FQDN** field.
   - Enter the root directory in the **Root Directory** field.
   - Enter the user name in the **User name** field.
   - Enter the password in the **Password** field.

4. Click **Apply**.

Configuring Backup settings

The Avaya Fabric Orchestrator (AFO) uses an external backup repository for additional storage of configuration files, and other backup files. Use this procedure to configure backup settings. Before and after you upgrade your Avaya Fabric Orchestrator (AFO) system, perform backup of the application related data, common services, and platform data. If an error occurs, use backup configuration files to return the AFO to a previous state.

Avaya recommends that you keep several copies of backup files. For more information, see About AFO Backup on page 138.

Procedure

1. On the **MSC Preference** page, click **Backup** tab.

   The system displays the **Backup** pane.

2. On the **External backup repository** section:

   Choose any one :

Choice Option	Choice Description
SCP	Select Secure Copy Protocol (SCP) for transferring files across a secure network.
FTP	Select File Transfer Protocol (FTP).

   - Enter the backup directory path in **Backup directory** field.

3. Click **Apply**.

Configuring Logging settings

Use log files and messages to perform diagnostic and fault management functions.

Use this procedure to configure the settings related to the external syslog server details, the protocol to use, purge parameters during Logging, and Log Harvesting tasks.

For more information about Logging and Log Harvesting, see Understanding Logging on page 124.

Procedure

1. On the **MSC Preference** page, click **Logging** tab.

   The system displays the **Logging** pane.

2. On the **External logging repository** section, select any one:

Choice Option	Choice Description
SCP	Select Secure Copy Protocol (SCP) for transferring files across a secure network.
FTP	Select File Transfer Protocol (FTP).

3. On the **External Syslog Server** section:

   - Enter the server IP address or FQDN name in the **Server IP/FQDN** field.

4. On the **Log Purge** section:
    - Select the retention limit threshold value in MB for the log archive files in the combo boxes.
5. On the **Log Purge Scheduler** section, select one of the Log Purge scheduler options:

Choice Option	Choice Description
Every Month On	Select a date to schedule Log Purge on a monthly basis.
Every Week On	Select a day to schedule Log Purge on a weekly basis.
Every Day	Select a time to schedule Log Purge on a daily basis.

6. Click **Apply**.

Chapter 8: EDM

Enterprise Device Manager

The following chapter contains conceptual and configuration information for Enterprise Device Manager (EDM) on Avaya Fabric Orchestrator (AFO).

Plugins inventory

The EDM plugin is a device plugin for a device version, or type, that you can install on an installed Avaya Fabric Orchestrator (AFO) base. You can install plugins on a base or advanced license. The network administrator and SMGR system administrator can perform the plugin management. You can install, uninstall, or view the EDM plugin by accessing the plugins inventory, from the navigation pane, under **Administration** > **Device Plug-in Management**.

AFO displays the EDM Plugin Inventory with a table containing all the installed plugins on the AFO server. Each row in the table depicts an EDM plugin, which specifies which device type and version is run with the plugin, as well as a list of supported device names.

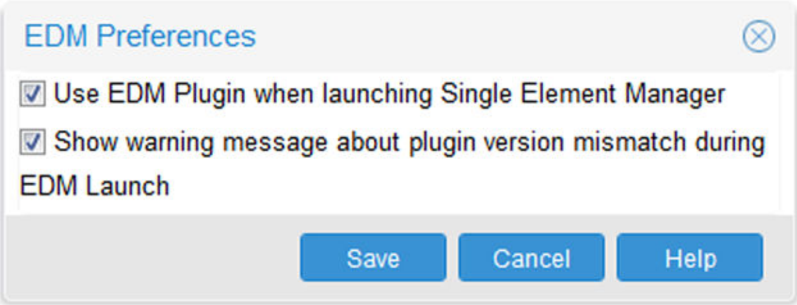
EDM plugins offer device management capabilities. Therefore, if you want to perform QoS / Filters operation on a particular device, then you can manipulate this functionality from the Element Manager for this device. The Element Manager for the EDM plugins is a browser-based solution that is launched through **Configuration** > **Network Map** or from **Configuration** > **Network Table**. To launch the Element Manager, right-click on a device, and select **Launch Element Manager** from the context menu. The EDM plugins are reused from the embedded EDM, or Element Manager, that is available in all the devices.

EDM Preferences

When EDM is launched on a device whose software version is not compatible with the version of the installed plugin, an EDM plugin version mismatch window displays, by default.

You can bypass the systematic logging of the message window.

In the navigation panel, go to **Administration** > **Device Plug-in Management**. Select EDM Preferences, on the top-left toolbar, and clear the **Show warning message about plugin version mismatch during EDM Launch** check box to bypass the systematic logging of the message window.



EDM Preferences

☑ Use EDM Plugin when launching Single Element Manager

☑ Show warning message about plugin version mismatch during EDM Launch

Important:

If you clear the **Use EDM Plugin when launching Single Element Manager** check box, the device may have performance issues.

Downloading EDM plugin

Perform the following procedure to download an EDM plugin.

Note:

Use Firefox to download EDM plugin from the Avaya support site to the Avaya Fabric Orchestrator (AFO) server.

Procedure steps

1. Open a web browser, and go to the Avaya support website: http://support.avaya.com.
2. Select Support by Product.
3. In the Enter Product Name, type `Enterprise Device Manager`, or choose `E` from the A-Z List, and then select `Enterprise Device Manager`.
4. Select the **Downloads** tab to view the latest EDM Plug-ins.
5. Download **EDM Plugin** for a specific device type and version.
6. Click **Save** to save the plugin file on to disk, where you are running the web browser.

Installing EDM plugin

Perform the following procedure to install an EDM plugin on Avaya Fabric Orchestrator (AFO).

Prerequisites

- You must have network administrator role or SMGR system administrator role rights to access the plugins Inventory.
- Ensure that you log on to AFO as an administrator.

Procedure Steps

1. Download the **EDM plugin** using the procedure, Downloading EDM plugin on page 67.

2. From the navigation pane, select **Administration** > **Device Plug-in Management**.
3. Click **Install Plugin**, which is the plus sign on the top left toolbar.

   The Plugin Install window displays.
4. To select the EDM Plugin file, click **Browse**.
5. Browse to the EDM plugin file, and then click **Open**.

   The file displays in the EDM Plugin file field.
6. To reset the EDM Plugin file, click **Reset**.
7. Click **Install**.

   If the installation is successful, the plugin appears in the EDM Plugins Inventory table or an error message displays describing the problem.

Installing required EDM plugins

EDM plugins are available at `/opt/avaya/smgr/com/EDMPlugins` on the MSC server.

AFO look ups the device inventory and then locates the corresponding EDM plugin in the repository.

Before you begin

- You must have network administrator role or UCM system administrator role rights to access plugins Inventory.
- Ensure that you log on to AFO as an administrator.
- AFO has discovered your network and the inventory shows all of your devices.

About this task

Perform the following procedure to install the required EDM plugins from the plugins bundle.

Procedure

1. From the navigation pane, select **Administration** > **Device Plug-in Management**.
2. Click the down arrow to the right of the **Add** button, and then select **Install required plugins**.
3. Click **Yes** in the confirmation window.

   If the installation is successful, the plugin displays in the EDM Plugin Inventory table or an error message displays describing the problem.

Uninstalling EDM plugin

Perform the following procedure to uninstall an EDM plugin from Avaya Fabric Orchestrator (AFO).

Prerequisites

- You must have network administrator role or SMGR system administrator role rights to access the plugins Inventory.

- Ensure that you log on to AFO as an administrator.

Procedure Steps

1. From the navigation pane, select **Administration** > **Device Plug-in Management**.
2. From the EDM Plugins Inventory table, select the plugin that you want to uninstall.
3. Click **Uninstall Plugin**, which is the minus sign on the top-left toolbar.
4. Click **Yes**.

   If the uninstall is successful, AFO displays the following message: EDM plugin uninstall successful. If the uninstall is not successful, AFO displays an error message that describes the problem.

Uninstalling unused EDM plugins

Perform the following procedure to uninstall unused EDM plugins. Use the following procedure for the Avaya Fabric Orchestrator (AFO) to look up the device inventory, and then locate any unused EDM plugins.

Before you begin

- You must have network administrator role or UCM system administrator role rights to access EDM Plugins Inventory.
- Ensure that you log on to AFO as an administrator.
- AFO has discovered your network and the inventory shows all of your devices.

Procedure

1. From the navigation pane, select **Administration** > **Device Plug-in Management**.
2. From the EDM Plugins Inventory table, select the plugin that you want to uninstall.
3. Click **Uninstall** and then click **Uninstall unused plugins**.
4. Click **Yes**.

   If the uninstall is successful, AFO displays `Plugins uninstall successful`.

   If the uninstall is not successful, AFO displays an error message that describes the problem.

Refreshing the plugin inventory table

Perform the following procedure to refresh the plugin inventory table.

Prerequisites

- You must have AFO System Administrator or AFO Network Administrator role rights to access the Plugins Inventory.
- Ensure that you log on to AFO as an administrator.

Procedure Steps

1. Download **EDM plugin** using the procedure, Downloading EDM plugin on page 67.
2. From the navigation pane, select **Administration** > **Device Plug-in Management**.
3. From the toolbar, click **Refresh Plugin Inventory**.

Chapter 9: vEDM

Virtual Enterprise Device Manager

This section provides concepts and procedures to configure Virtual Enterprise Device Manager (vEDM).

Virtual Enterprise Device Manager

This section provides fundamental concepts for Virtual Enterprise Device Manager (vEDM).

Virtual EDM

Virtual Enterprise Device Manager (vEDM) allows users to visualize the association of bridges, ports, and interfaces of the open virtual switch.

You can use vEDM to debug the system by visualizing bridges, ports and interfaces associations, when users change the network configuration, or properties of these components that are modified through Command Line Interface (CLI).

The vEDM feature is modelled after Enterprise Device Manager (EDM), which is a graphical user interface used to configure Avaya switches.

The vEDM feature enables you to:

- Visualize the virtual components of the open virtual switch.
- Associate bridges, ports, and interfaces with each other.

Virtual EDM (vEDM) requires AFO installation. You must be logged into Avaya Fabric Orchestrator (AFO), and launch vEDM from the AFO menu bar.

You launch vEDM through the AFO menu bar, through **Administration** > **vEDM**.

vEDM components

The vEDM feature configures the Open Virtual Switch Database (OVSDB), and consists of three components:

- vEDM web server
- vEDM application browser client
- Open Virtual Switch Database

How it works

The client (vEDM application browser) sends or receives to the vEDM server, and then the vEDM server sends or receives to the Open Virtual Switch Database.

Device Logical View

After you launch the vEDM feature, you immediately see the Device Logical View, which displays a topology like graph. The Device Logical View displays:

- The relationship between the bridges and their respective ports and interfaces.
- A legend that represents the type of component.

In the Device Logical View, a red line between a port and interface indicates that the interface connected to a port is a local virtual interface. The interface is created by default when a port is created.

Bonded ports are those that have more than one interface associated to the same port. A minimum of two physical interfaces are required to create a bonded port.

Link aggregation, also known as interface bonding, joins multiple physical interfaces together into a virtual interface, known as a bond interface. A bond interface is generally configured for High Availability redundancy, or for loading sharing, which increases connection throughput above that which is possible using one physical interface.

OVSDB

The Open Virtual Switch Database (OVSDB) tab displays a summary of this Open Virtual Switch Database. You can use the **Refresh** button to update **OVSDB** tab information, but the information is read-only.

Bridge tab

The Bridge tab displays bridges configured in the Open Virtual Switch, and attributes of each bridge. The information displayed is read-only. You can export or print the bridge tab table information, as well as refresh the content.

Port tab

The **Port** tab displays all virtual information of the ports. The information displayed is read-only. You can export or print the port tab table information, as well as refresh the content.

Interface tab

The Interface tab displays all the interfaces present in the AFO appliance, both physical and virtual. The information displayed is read-only. You can export or print the interface tab table information, as well as refresh the content.

vEDM limitations

This section describes the restrictions and limitations associated with vEDM.

- The vEDM feature only supports bridge, port, and interface tables for the current release.
- All operations are read-only.
- Tabs within the application do not communicate with each other. If you make updates to one table, you must refresh the other associated tables to see the update.

Virtual EDM device support

Virtual EDM (vEDM) requires AFO 1.0 installation.

For more information on supported Avaya devices see *Deploying Avaya Fabric Orchestrator*, NN48100–101.

vEDM configuration

This section provides configuration information for Virtual Enterprise Device Manager (vEDM).

Viewing the vEDM Device Logical View

After you launch the vEDM feature, you immediately see the Device Logical View, which displays a topology like graph. The Device Logical View displays:

- The relationship between the bridges and their respective ports and interfaces.
- A legend that represents the type of component.

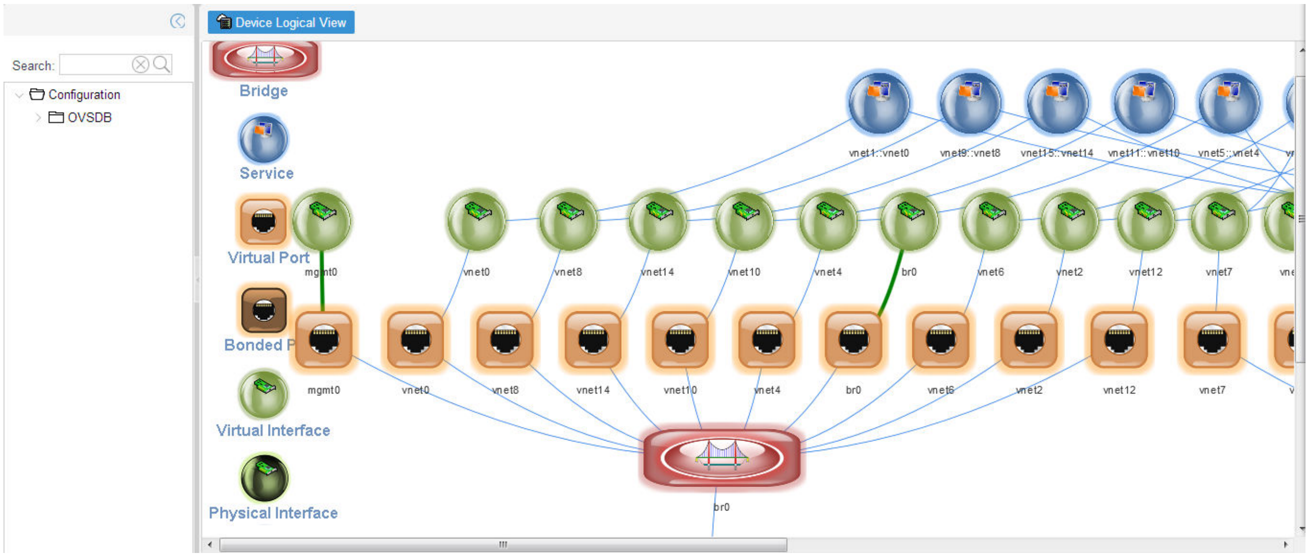
Before you begin

- The vEDM feature requires Avaya Fabric Orchestrator (AFO) installation.
- You must be logged in to AFO.

Procedure

On the menu bar, click **Administration** > **vEDM** to start **vEDM**.

The Device Logical View displays.



vEDM field descriptions

Use the data in the following table to use the **Device Logical View** tab.

Name	Description
Bridge	Specifies a switch with one or more ports.
Service	Specifies a switch running one or more services.
Virtual Port	Specifies a virtualized representation of a port.
Bonded Port	Specifies a bonded port, which means a port that has more than one interface associated to the same port. A minimum of two physical interfaces is required to create a bonded port.
Virtual Interface	Specifies a virtualized representation of a computer network interface.
Physical Interface	Specifies an actual physical computer network interface.

Viewing the Open Virtual Switch Database information

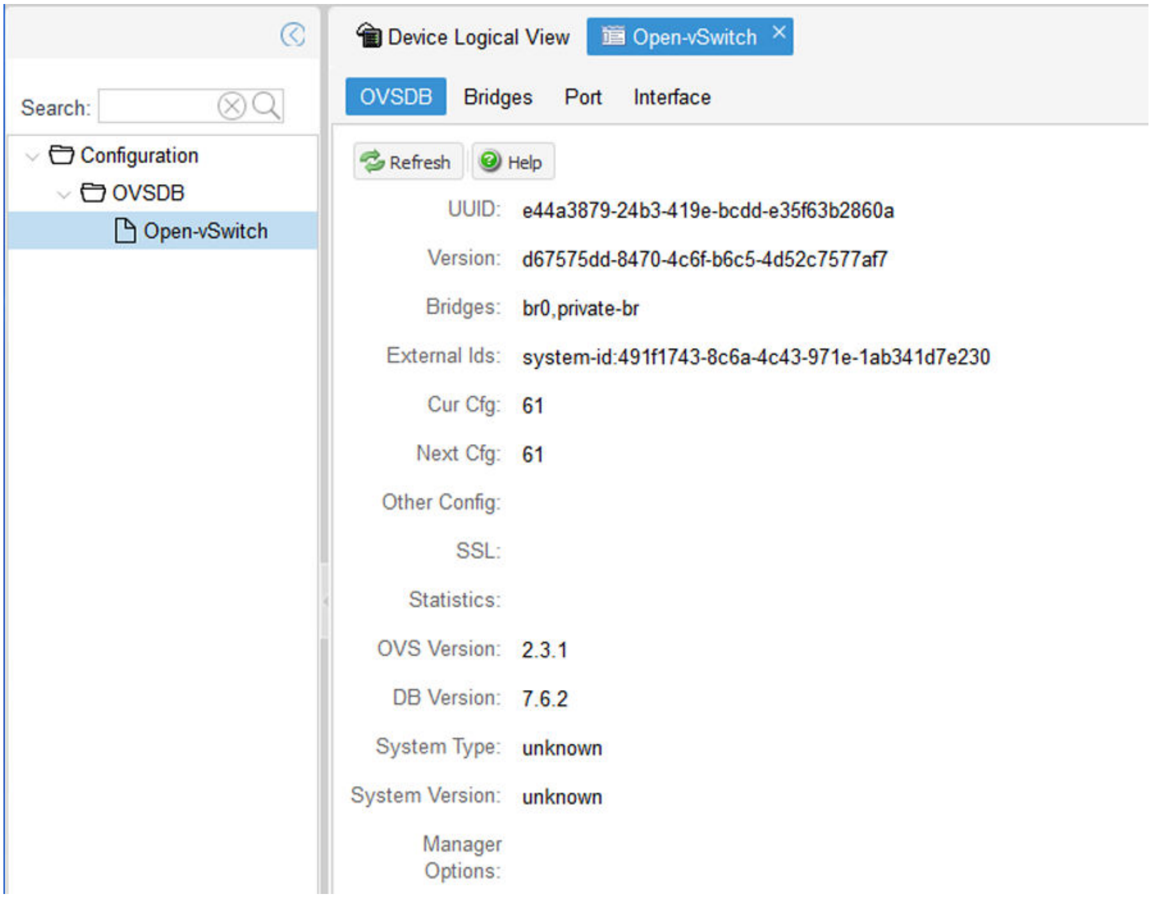
Use this procedure to view a summary of this Open Virtual Switch Database (OVSDB) information.

Before you begin

- The vEDM feature requires Avaya Fabric Orchestrator (AFO) installation.
- You must be logged in to AFO.

Procedure

1. On the menu bar, click **Administration** > **vEDM** to start **vEDM**.
2. Select **Configuration** > **OVSDB** > **Open-vSwitch**.
3. Select the **OVSDB** tab to view Open Virtual Switch Database information.



UUID: e44a3879-24b3-419e-bcdd-e35f63b2860a

Version: d67575dd-8470-4c6f-b6c5-4d52c7577af7

Bridges: br0,private-br

External Ids: system-id:491f1743-8c6a-4c43-971e-1ab341d7e230

Cur Cfg: 61

Next Cfg: 61

Other Config:

SSL:

Statistics:

OVS Version: 2.3.1

DB Version: 7.6.2

System Type: unknown

System Version: unknown

Manager Options:

OVSDB tab field descriptions

Use the data in the following table to use the **OVSDB** tab.

Note:

All fields in the OVSDB tab are read-only.

Name	Description
UUID	Specifies a unique identifier for the physical host.
Version	Specifies the Open vSwtich version.
Bridges	Specifies a set of bridges managed by the system.
External Ids	Specifies a unique identifier for the physical host of the Open Virtual Switch. The form of the identifier depends on the type of host.
Cur Cfg	Specifies a sequence number that the Open Virtual Switch sets to the current value of the Next cfg after it finishes applying a set of configuration changes.
Next Cfg	Specifies a sequence number for the client to increment. When the client modifies any part of the

Table continues…

Name	Description
	database configuration and wants to wait for the Open Virtual Switch to finish applying the changes, it can increment this sequence number.
Other Config	Specifies the interval for updating statistics to the database in milliseconds (ms). This option will affect the update of the statistics column in the following tables: Port and Interface. The default is 5000 ms.
SSL	Specifies if the system uses Secure Socket Layer (SSL). This is an optional field.
Statistics	Specifies key-value pairs that report statistics about the system running an Open Virtual Switch. Statistics are updated periodically.
OVS Version	Specifies the Open Virtual Switch version number.
DB version	Specifies the database schema version number in the form of major change, minor change, tweak change, as <major.minor.tweak> numerically as for instance 2.1.3, which would denote two major releases, one minor release, and three tweaks. Whenever the database schema is changed in a non-backward compatible way, then it is a major release change. When the database is changed in a backward compatible way it is a minor release change. When the database is changed cosmetically it is a tweak release change.
System Type	Specifies an identifier for the type of system on top of which the Open Virtual Switch runs.
System Version	Specifies the version of the system.
Manager Options	Specifies the database clients to which the Open Switch Database server connects or to which it listens, along with the options for how these connections are configured.

vEDM bridge configuration

Use the following procedures to view and export the vEDM bridge configuration. A bridge record represents an Ethernet switch with one or more ports.

Viewing the vEDM bridge configuration

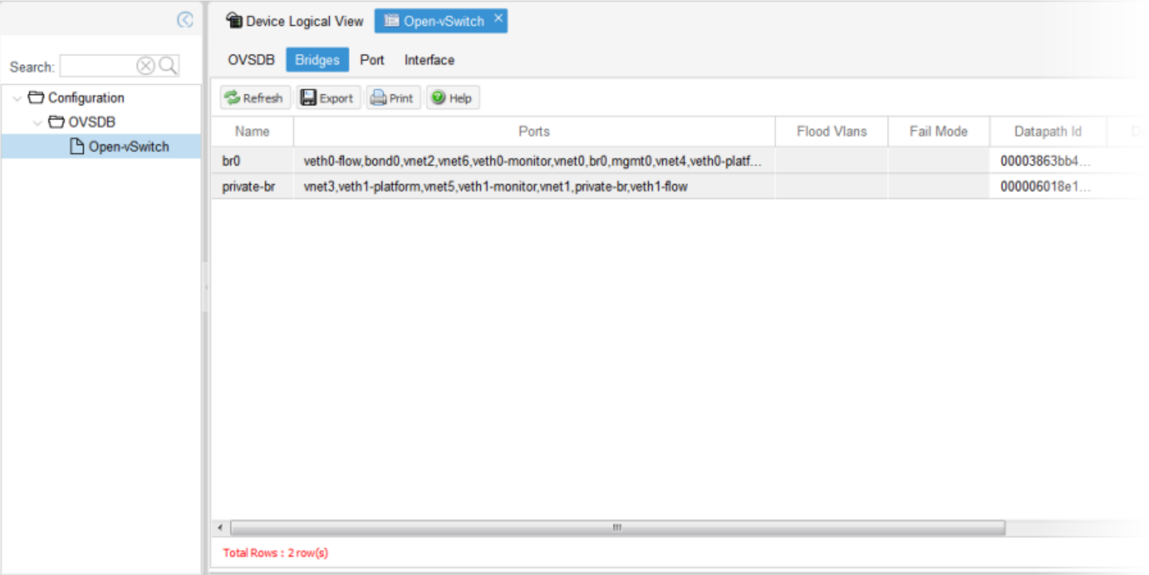
Use this procedure to view the vEDM bridge configuration. A bridge record represents an Ethernet switch with one or more ports.

Before you begin

- The vEDM feature requires Avaya Fabric Orchestrator (AFO) installation.
- You must be logged in to AFO.

Procedure

1. On the menu bar, click, select **Administration** > **vEDM** to start **vEDM**.
2. Select **Configuration** > **OVSDB** > **Open-vSwitch**.
3. Select the **Bridges** tab.



Name	Ports	Flood Vlans	Fail Mode	Datapath Id
br0	veth0-flow,bond0,vnet2,vnet6,veth0-monitor,vnet0,br0,mgmt0,vnet4,veth0-platf...			00003863bb4...
private-br	vnet3,veth1-platform,vnet5,veth1-monitor,vnet1,private-br,veth1-flow			000006018e1...

Total Rows : 2 row(s)

4. **(Optional)** If you want to refresh the table, click **Refresh**.

Bridge tab field descriptions

Use the data in the following table to use the **Bridge** tab.

Note:

All fields in the Bridge tab are read-only.

Name	Description
Name	Specifies the bridge name. The name must be unique within the table. The bridge name must be alphanumeric and no more than 8 bytes long.
Ports	Specifies all of the ports on the bridge.
Flood VLANs	Configures up to 4,096 integers in a range of 0 to 4,095 VLAN IDs on which you must disable MAC address learning.
Fail Mode	Specifies the fail mode as either: • secure—In secure mode, the Open Virtual Switch will not set up flows on its own when the controller connection fails or when no controllers are defined. The bridge will continue to retry connecting to any defined controllers forever.

Table continues…

Name	Description
	• standalone—In standalone mode, if no message is received from the controller for three times, the inactivity probe interval, then the Open Virtual Switch takes over responsibility for setting up flows. In this mode, the Open Virtual Switch causes the bridge to act like an ordinary MAC-learning switch. The Open Virtual Switch continues to retry connecting to the controller in the background, and when the connection succeeds it discontinues its standalone behavior. When a controller is configured normally it is responsible for setting up all flows on the switch, so if the connection to the controller fails, then no new network connections can be set up. If the connection to the controller stays down long enough, no packets can pass through the switch at all. This setting determines the response of the switch to such a situation. The standalone mode can create forwarding loops on a bridge that has more than one uplink port unless STP is enabled. To avoid ops on such a bridge, configure secure mode or enable STP. When more than one controller is configured, fail mode is considered only when none of the configured controllers can be contacted. This is optional parameter. If the value is not configured, the default is standalone.
Datapath Id	Specifies the Open Flow datapath ID in exactly 16 hexadecimal digits. This is an optional parameter.
Datapath Type	Specifies the datapath provider. The kernal datapath has type system. The userspace datapath has type netdev.
Protocols	Specifies the protocol as one of the following: • OpenFlow11 • OpenFlow10 • OpenFlow13 • OpenFlow12 • OpenFlow15 • Open-Flow14 This is an optional parameter.

Table continues…

Name	Description
	If this column is empty, OpenFlow 1.0, 1.1, 1.2, and 1.3 are enabled by default.
STP Enable	Enables spanning tree on the bridge. By default, STP is disabled on bridges. Bond, internal, and mirror ports are not supported and will not participate in the spanning tree.
Status	Specifies the status of bridges.
External Ids	Specifies key-value pairs for use by external faremworks that integrate with Open vSwitch, rather than by Open vSwitch itself.
Other Config	Specifies key-value pairs for configuring rarely used features.

Exporting bridge information with vEDM

Use this procedure to export bridge information with vEDM. A bridge record represents an Ethernet switch with one or more ports.

Before you begin

- The vEDM feature requires Avaya Fabric Orchestrator (AFO) installation.
- You must be logged in to AFO.

Procedure

1. On the menu bar, click **Administration** > **vEDM** to start **vEDM**.
2. Select **Configuration** > **OVSDB** > **Open-vSwitch**.
3. Select the **Bridges** tab.
4. Click **Export** to export the information to a separate web page.
5. Save the information from your web browser as an HTML file.
6. If you want to print the **Bridges** tab information, click **Print**.
7. Select the printer name you want to use.
8. Click **OK**.

vEDM port configuration

Use the following procedures to view the vEDM port configuration.

Viewing the vEDM port configuration

Use this procedure to view the vEDM port configuration. Usually a port within a bridge has one interface pointed to it by its interfaces column. Such a port logically corresponds to a port on a physical Ethernet switch. A port with more than one interface is a bonded port.

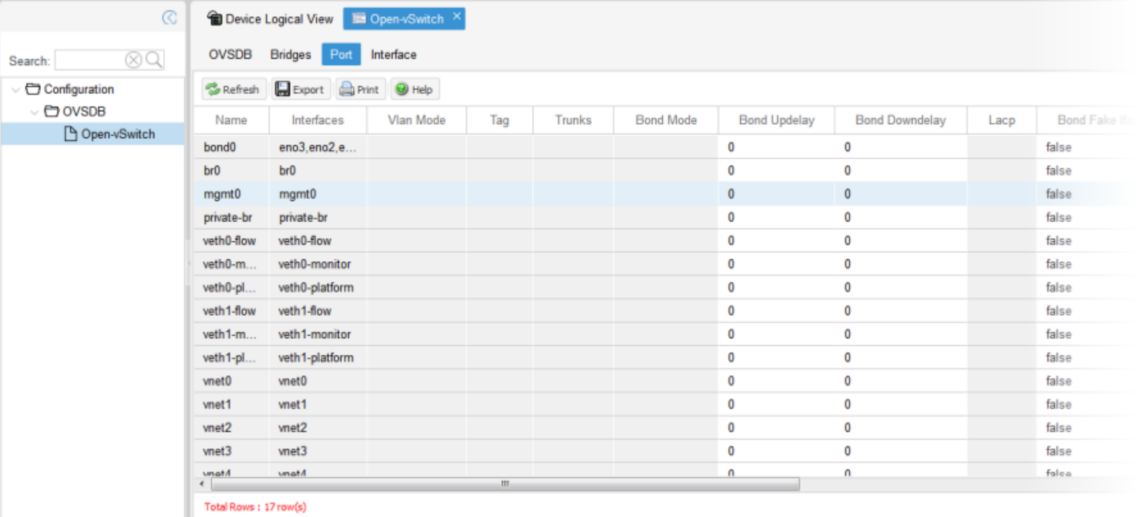
Before you begin

- The vEDM feature requires Avaya Fabric Orchestrator (AFO) installation.

- You must be logged in to AFO.

Procedure

1. On the menu bar, click **Administration** > **vEDM** to start **vEDM**.
2. Select **Configuration** > **OVSDB** > **Open-vSwitch**.
3. Select the **Port** tab.



Name	Interfaces	Vlan Mode	Tag	Trunks	Bond Mode	Bond Updelay	Bond Downdelay	Lacp	Bond Fake
bond0	eno3,eno2,e...					0	0		false
br0	br0					0	0		false
mgmt0	mgmt0					0	0		false
private-br	private-br					0	0		false
veth0-flow	veth0-flow					0	0		false
veth0-m...	veth0-monitor					0	0		false
veth0-pl...	veth0-platform					0	0		false
veth1-flow	veth1-flow					0	0		false
veth1-m...	veth1-monitor					0	0		false
veth1-pl...	veth1-platform					0	0		false
vnet0	vnet0					0	0		false
vnet1	vnet1					0	0		false
vnet2	vnet2					0	0		false
vnet3	vnet3					0	0		false
vnet4	vnet4					0	0		false

Total Rows : 17 row(s)

4. **(Optional)** If you want to refresh the table, click **Refresh**.

Port tab field descriptions

Use the data in the following table to use the **Port** tab.

Note:

All fields in the **Port** tab are read-only.

Name	Description
Name	Specifies the port name, which is an immutable string, which must be unique within the table. The name should be alphanumeric and no more than 8 bytes long. The name may be the same as the interface name for non-bonded ports; otherwise the name must be unique among the names of ports, interfaces, and bridges on a host.
Interfaces	Specifies the interfaces of the port. If there is more than one interface associated with the port, the port is a bonded port.
Vlan Mode	Specifies the VLAN mode of the port, as one of the following: • access

Table continues…

Name	Description
	• native-tagged • native-untagged • trunk This is an optional parameter. If this column is empty, the default mode is selected as follows: 1. If the tag contains a value, the port is an access port. The trunks column should be empty. 2. Otherwise, the port is a trunk port. The trunks column value is honored if it is present.
Tag	Specifies a value in the range of 0 to 4,095. For an access port, the port is an implicitly tagged VLAN. For a native-tagged or native-untagged port, the port is a native VLAN. This value must be empty if this is a trunk port. This is an optional parameter.
Trunks	Specifies the 802.1Q VLAN or VLANs that this port trunks for native-tagged, or native-untagged ports in a value in a range of 0 to 4,095. If the value is empty, then the port trunks are all VLANs. This value must be empty if this is an access port. A native-tagged or native-untagged port always trunks its native VLAN, regardless of whether trunks includes that VLAN.
Bond Mode	Specifies the type of bonding for a bonded port, as one of the following: • active-backup • balance-tcp • balance-slb The default is active-backup.
Bond Updelay	Specifies the number of milliseconds for which the link must stay up on an interface before the interface is considered to be up. Specify 0 to enable the interface immediately. This setting is honored only when at least one bonded interface is already enabled. When no interfaces are enabled, then the first bond interface to come up is enabled immediately.

Table continues…

Name	Description
Bond Downdelay	Specifies the number of milliseconds for which the link must stay down on an interface before the interface is considered to be down. Specify 0 to disable the interface immediately.
Lacp	Configures Link Aggregation Control Protocol (LACP) on this port, as one of the following: • active—Active ports are allowed to initiate LACP negotiations. • passive—Passive ports are allowed to participate in LACP negotiations initiated by a remote switch, but not allowed to initiate such negotiations themselves. • off LACP allows directly connected switches to negotiate which links may be bonded. LACP may be enabled on non-bonded ports for the benefit of any switches they may be connected to. If LACP is enabled on a port whose partner switch does not support LACP, the bond will be disabled, unless other-config:lacp-fallback-ab is configured to true. The default is off.
Bond Fake Iface	For a bonded port, specifies whether to create a fake internal interface with the name of the port. Use this parameter only for compatibility with legacy software that requires this.
Bond Active Slave	For a bonded port, the field records the MAC address of the current active slave.
Qos	Specifies the Quality of Service (QoS) configuration for this port.
Mac	Specifies the MAC address to use for this port for the purpose of choosing the MAC address of the bridge. This column does not necessarily reflect the actual MAC address of the port, and if you configure a different MAC address it does not change the actual MAC address of the port.
Fake Bridge	Specifies if this port represents a sub-bridge for its tagged VLAN within the bridge.
External Ids	Specifies key-value pairs for use by external frameworks that integrate with Open vSwitch, rather than by Open vSwitch itself.
Status	Specifies the status of ports attached to bridges.

Table continues…

Name	Description
Other Config	Specifies key-value pairs for configuring rarely used features.

Exporting the port information with vEDM

Use this procedure to configure a port with vEDM. Usually a port within a bridge has one interface pointed to it by its interfaces column. Such a port logically corresponds to a port on a physical Ethernet switch. A port with more than one interface is a bonded port.

Before you begin

- The vEDM feature requires Avaya Fabric Orchestrator (AFO) installation.
- You must be logged in to AFO.

Procedure

1. On the menu bar, click **Administration** > **vEDM** to start **vEDM**.
2. **Configuration** > **OVSDB** > **Open-vSwitch**.
3. Select the **Port** tab.
4. Click **Export** to export the information to a separate web page.
5. Save the information from your web browser as an HTML file.
6. If you want to print the **Port** tab information, click **Print**.
7. Select the name of the printer you want to use.
8. Click **OK**.

vEDM interface configuration

Use the following procedures to view the vEDM interface configuration.

Viewing the vEDM interface

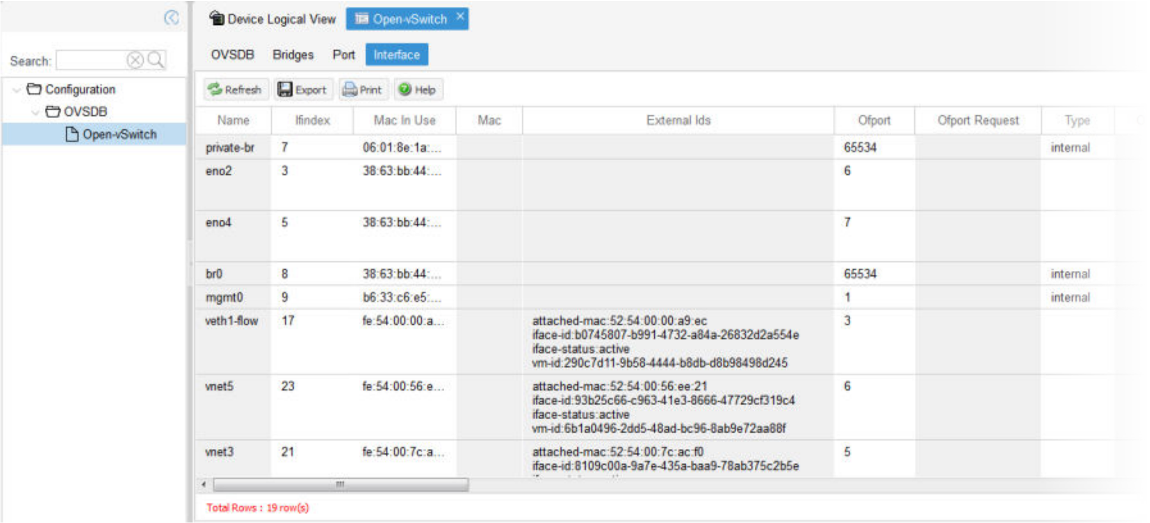
Use this procedure to view the vEDM interface.

Before you begin

- The vEDM feature requires Avaya Fabric Orchestrator (AFO) installation.
- You must be logged in to AFO.

Procedure

1. On the menu bar, click **Administration** > **vEDM** to start **vEDM**.
2. Select **Configuration** > **OVSDB** > **Open-vSwitch**.
3. Select the **Interface** tab.



Name	Ifindex	Mac In Use	Mac	External Ids	Ofport	Ofport Request	Type
private-br	7	06:01:8e:1a:...			65534		internal
eno2	3	38:63:bb:44:...			6		
eno4	5	38:63:bb:44:...			7		
br0	8	38:63:bb:44:...			65534		internal
mgmt0	9	b6:33:c6:e5:...			1		internal
veth1-flow	17	fe:54:00:00:a...		attached-mac:52:54:00:00:a9:ec iface-id:b0745807-b991-4732-a84a-26832d2a554e iface-status:active vm-id:290c7d11-9b58-4444-b8db-d8b98498d245	3		
vnet5	23	fe:54:00:56:e...		attached-mac:52:54:00:56:ee:21 iface-id:93b25c66-c963-41e3-8666-47729cf319c4 iface-status:active vm-id:6b1a0496-2dd5-48ad-bc96-8ab9e72aa88f	6		
vnet3	21	fe:54:00:7c:a...		attached-mac:52:54:00:7c:ac:f0 iface-id:8109c00a-9a7e-435a-baa9-78ab375c2b5e	5		

Total Rows : 19 row(s)

4. **(Optional)** If you want to refresh the table, click **Refresh**.

Interface tab field descriptions

Use the data in the following table to use the **Interface** tab.

Note:

All fields in the **Interface** tab are read-only.

Name	Description
Name	Specifies the interface name, which is an immutable string that must be unique within the table. The name must be alphanumeric, and no more than 8 bytes long. The interface name may be the same as the port name, for non-bonded ports, otherwise the interface name must be unique among the names of ports, interfaces, and bridges on a host.
IfIndex	Specifies a positive interface index, as defined for SNMP MIB-II in RFCs 1213 and 2863. The value is an optional integer,in the range of 0 to 4,294,967,295. If the interface has a value, otherwise the value is 0. The ifindex is useful for seamless integration with protocols such as SNMP and sFlow
Mac in Use	Specifies the MAC address in use by this interface. This is an optional parameter.
Mac	Specifies the Ethernet address to configure for this interface.

Table continues…

Name	Description
	If this value is not configured, then the default MAC address is used: • The local interface default is the lowest-numbered MAC address among the other bridge ports, either the value of the MAC in its port record, if configured, or its actual MAC (for bonded ports, the MAC of its secondary interface whose name is first in alphabetical order). Internal ports and bridge ports that are used as port mirroring destinations are ignored. • The default for other internal interfaces is randomly generated. • External interfaces typically have a MAC address associated with their hardware. Some interfaces may not have a software-controllable MAC address. This is an optional parameter.
Ofport	Specifies the OpenFlow port number for this interface. The Open Virtual Switch configures the value of this column. The OpenFlow ‘local’ port is 65,534. The other valid port numbers are in the range 1 to 65,279, inclusively. The value −1 indicates an error occurred adding this interface This is an optional parameter.
Ofport Request	Specifies the requested OpenFlow port number for this interface in range of 1 to 65,279. A client should ideally set the value of this column during the same database transaction as when the client creates the interface. The Open Virtual Switch version 2.1 and later honors a later request for a specific port number, although it might confuse some controllers. OpenFlow does not have a way to announce a port number change, so the Open Virtual Switch represents the change over OpenFlow as a port deletion followed immediately by a port addition. If the Ofport Request is set or changed to the automatically assigned port number of some other port, then Open Virtual Switch chooses a new port number for the latter port. This is an optional parameter.

Table continues…

Name	Description
Type	Specifies the interface type, as one of the following: • system—Specifies an ordinary network device, which is sometimes referred to as external interfaces since they are generally connected to hardware external to that on which the Open Virtual Switch is running. The empty string is a synonym for the system. • internal—Specifies a simulated network device that sends and receives traffic. An internal interface whose name is the same as the name of its bridge is called the local interface. It does not make sense to bond an internal interface, so the terms port and interface are often used imprecisely for internal interfaces. • tap—Specifies a TUN/TAP device managed by Open vSwitch.
Options	Specifies the options that apply to interfaces with type of: • geneve—Specifies an Ethernet over Geneve IPv4 tunnel. Geneve supports options as a means to transport additional metadata; however, currently only the 24-bit VNI is supported. This is planned to be extended in the future. • gre—Specifies an Ethernet over RFC 2890 Generic Routing Encapsulation over IPv4 tunnel. • ipsec_gre—Specifies an Ethernet over RFC 2890 Generic Routing Encapsulation over IPv4 IPsec tunnel. • gre64—Specifies the same thing as GRE, except that gre64 allows a 64-bit key. For gre64 to store higher than 32-bits of key, it uses the GRE protocol sequence number field. This is a nonstandard use of the GRE protocol since Open Virtual Switch does not increment the sequence number for every packet at the time of encapsulation, as expected by the standard GRE implementation. • ipsec_gre64—Specifies the same as IPSEC_GRE except that it allows for a 64-bit key. • vxlan—Specifies an Ethernet tunnel over the experimental, UDP-based VXLAN. Open Virtual Switch uses UDP destination port 4789. The source port used for VXLAN traffic varies on a per-flow basis and is in the ephemeral port range. • lisp—Specifies a layer 3 tunnel over the experimental, UDP-based Locator/ID Separation

Table continues…

Name	Description
	Protocol (RFC6830).Only IPv4 and IPv6 packets are supported by the protocol, and they are sent and received without an Ethernet header. Traffic to and from LISP ports is expected to be configured explicitly, and the ports are not intended to participate in learning based switching. As such, they are always excluded from packet flooding.
Admin State	Specifies the administrative state of the physical network link. This is an optional parameter, either up or down.
Link State	Specifies the observed state of the physical network link. This is ordinarily the carrier status of the link. If the port of the interface is a bond configured for MII link monitoring in milliseconds, it is instead the MII monitoring status of the network link. This is an optional parameter, either up or down.
Link Resets	Specifies the number of times the Open Virtual Switch has observed the link state of this Interface change. This is an optional parameter.
Link Speed	Specifies the negotiated speed of the physical network link. The valid values are positive integers greater than 0. This is an optional parameter.
Duplex	Specifies the duplex mode of the physical network link.
Mtu	Specifies the maximum transmission unit (MTU), which is the largest amount of data that can fit into a single Ethernet frame. The standard MTU is 1500 bytes. You can configure some physical media and many kinds of virtual interfaces with higher MTUs. The column is empty for an interface that does not have an MTU, for example, some kinds of tunnels do not.
Lacp Current	Specifies the Link Aggregation Control Protocol (LACP) status for this interface. If true, this interface has current LACP information about its LACP partner. This information may be used to monitor the health of interfaces in an LACP enabled port. This column is empty if LACP is not enabled.
Status	Specifies key-value pairs that report port status.
Ingress Policing Burst	Specifies the maximum burst size for data received on this interface in kb. The default bust size, if

Table continues…

Name	Description
	configured to 0, is 1000 kb. This value has no effect if the Ingress Policing Rate is 0.
Ingress Policing Rate	Specifies the maximum rate for data received on this interface, in kbps. Data received faster than this rate is dropped. Configure this value to 0 to disable policing.
Bfd	Specifies Bidirectional Forwarding Detection (BFD). BFD allows point-to-point detection of connectivity failures by occasional transmission of BFD control messages. Open vSwitch implements BFD to serve as a more popular and standards compliant alternative to CFM. BFD operates by regularly transmitting BFD control messages at a rate negotiated independently in each direction. Each endpoint specifies the rate at which it expects to receive control messages, and the rate at which it can transmit them. Open vSwitch uses a detection multiplier of three, meaning that an endpoint signals a connectivity fault if three consecutive BFD control messages fail to arrive. In the case of a unidirectional connectivity issue, the system not receiving BFD control messages signals the problem to its peer in the messages it transmits.
Bfd Status	Reports the state of the BFD session. The BFD session is fully health and negotiated if the field displays as UP.
Cfm Fault	Indicates a connectivity fault triggered by an inability to receive heartbeats from any remote endpoint. When a fault is triggered on interfaces participating in bonds, the system disables those interfaces. Faults can be triggered for several reasons. Most importantly the system triggers faults when the system receives no CCMs for a period of 3.5 times the transmission interval. The system also triggers faults when any CCMs indicate that a Remote Maintenance Point does not receive CCMs but can send them. Finally, the system triggers a fault if the system receives a CCM which indicates and unexpected configuration. Notably, this case arises when the system receives a CCM which advertises the local MPID.
Cfm Fault Status	Specifies the Connectivity Fault Management (CFM) fault status as one of the following: • recv—Indicates the system triggered a CFM fault due to a lack of CCMs received on the Interface.

Table continues…

Name	Description
	• rdi—Indicates the system triggered a CFM fault due to the reception of a CCM with the RDI bit flagged. Endpoints set the RDI bit in their CCMs when they are not receiving CCMs themselves. This typically indicates a unidirectional connectivity failure. • maid—Indicates the system triggered a CFM fault due to the reception of a CCM with a MAID other than the one Open vSwitch uses. The system tags CFM broadcasts with an identification number in addition to the MPID called the MAID. Open vSwitch only supports receiving CCM broadcasts tagged with the MAID it uses internally. • loopback—Indicates the system triggered a CFM fault due to the reception of a CCM advertising the same MPID configured in the cfm_mpid column of this Interface. This may indicate a loop in the network. • overflow—Indicates the system triggered a CFM fault because the CFM module received CCMs from more remote endpoints than it can keep track of. • override—Indicates an administrator triggered a CFM fault manually through an ovs−appctl command. • interval—Indicates the system triggered a CFM fault due to the reception of a CCM frame having an invalid interval.
Cfm Flap Status	Specifies the CFM flap status.
Cfm Flap Count	Counts the number of CFM fault flaps since boot. A flap is considered to be a change of the cfm_fault value.
Cfm Health	Indicates the health of the interface as a percentage of CCM frames received over 21 other_config: cfm_intervals. The system does not define the health of an interface if the interface is communicating with more than one cfm_remote_mpids. It reduces if the system does not receive healthy heartbeats at the expected rate, and gradually improves as the system receives healthy heartbeats at the wanted rate. Every 21 other_config: cfm_intervals, the system refreshes health of the interface.

Table continues…

Name	Description
	As mentioned above, the system can trigger faults for several reasons.
Cfm Mpid	Specifies a maintenance point ID (MPID), which uniquely identifies each endpoint within a maintenance association. The MPID identifies this endpoint to other maintenance points in the MA. Each end of a link being monitored must have a different MPID, and must be configured to enable CFM on this interface. According to the 802.1ag specification, MPIDs can only range between [1, 8191]. However, extended mode (see other_config:cfm_extended) supports eight-byte MPIDs.
Cfm Remote Mpids	Specifies the list of MPIDs from which this interface receives broadcasts. The remote MPID information is regularly collected and written to this column. When CFM is properly configured, Open vSwitch occasionally receives CCM broadcasts. These broadcasts contain the MPID of the sending maintenance point.
Cfm Remote Opstate	When in extended mode, indicates the operational state of the remote endpoint as either up or down.
External Ids	Specifies key-value pairs for use by external faremworks that integrate with Open vSwitch, rather than by Open vSwitch itself.
Other Config	Specifies key-value pairs for configuring rarely used features.

Exporting the interface information with vEDM

Use this procedure to export interface information with vEDM.

Before you begin

- The vEDM feature requires Avaya Fabric Orchestrator (AFO) installation.
- You must be logged in to AFO.

Procedure

1. On the menu bar, click **Administration** > **vEDM** to start **vEDM**.
2. Select **Configuration** > **OVSDB** > **Open-vSwitch**.
3. Select the **Interface** tab.
4. Click **Export** to export the information to a separate web page.
5. Save the information from your web browser as an HTML file.
6. If you want to print the **Interface** tab information, click **Print**.

7. Select the printer name where you want the information to print.
8. Click **OK**.

Chapter 10: Appliance Device Manager (ADM)

This chapter provides concepts and procedures to configure Appliance Device Manager (ADM) on Avaya Fabric Orchestrator (AFO).

Appliance Device Manager Overview

This section describes the fundamental concepts for Appliance Device Manager (ADM).

ADM is primarily a monitoring and configuration web-based graphical user interface (GUI) application. ADM runs on your AFO appliance and co-resides within the Management Server Console (MSC) jboss container. ADM manages the AFO appliance and the services (virtual machines) present in the appliance. You can access ADM using one of the following supported Web browsers:

- Mozilla FireFox, versions 40, 41
- Microsoft Internet Explorer, versions 10, 11

To configure multiple devices through one interface, you can install Avaya Fabric Orchestrator Configuration (AFO Configuration) on a remote server. For more information about AFO Configuration documentation, see *Network Configuration using Avaya Fabric Orchestrator*, NN48100–501.

The ADM feature enables you to:

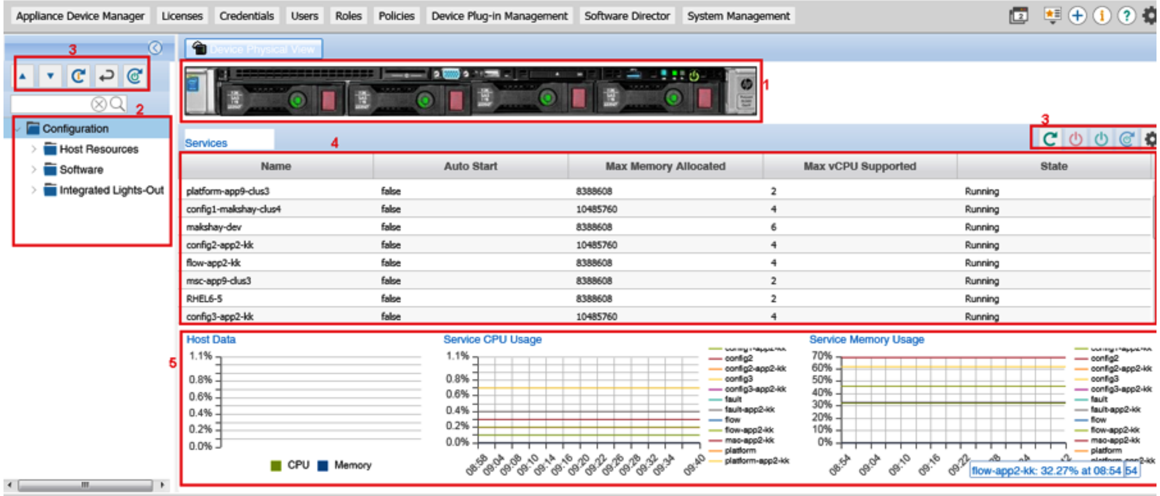
- Check the overall health status of the AFO appliance.
- Start, stop, and check status of the AFO service management.
- Launch Integrated Lights-Out (iLO).

Note:

You can also access ADM when the platform service is down, using the Management Server Console (MSC). For more information, see Access to ADM when platform service is down on page 98.

ADM Window

The ADM window displays the overall health and static data of the Avaya Fabric Orchestrator (AFO) appliance. Use ADM window to identify and troubleshoot issues. The following figure and table shows the different sections of the ADM window:



Name	Auto Start	Max Memory Allocated	Max vCPU Supported	State
platform-app9-clus3	false	8388608	2	Running
config1-makshay-clus4	false	10485760	4	Running
makshay-dev	false	8388608	6	Running
config2-app2-kk	false	10485760	4	Running
flow-app2-kk	false	8388608	4	Running
msc-app9-clus3	false	8388608	2	Running
RHEL6-5	false	8388608	2	Running
config3-app2-kk	false	10485760	4	Running

Figure 3: ADM window

1	Device Pane
2	Navigation Pane
3	Toolbar
4	Grid Pane
5	Monitoring Graphs

Device Pane

After you access ADM, the first screen displays the physical device view along with the overall health status of the AFO appliance. The top panel displays a real-time physical view of the front or back panel of the AFO.

You can use the **Flip** icon given at the top-left corner on the toolbar, to rotate the view as front or back. ADM physical device view indicates the status of the LEDs and the physical components of the KVM server; disks, power supply, and interfaces.

The conventions on the device view are similar to the actual device appearance. The module LEDs and the ports are color-coded to provide status. Green indicates the module or port is up and running, red indicates the module or port is disabled, and amber indicates an enabled port that is not connected to anything.

You can use the device view to determine the operating status of the various modules and ports in your hardware configuration. You can also use the device view to perform management tasks on specific objects.

Navigation Pane

Located to the left of the window, the navigation pane contains a directory tree structure that displays all the available configuration tabs. You can use the navigation pane to see what configurations are available and to quickly browse through the configuration hierarchy. You can use the toolbar above the navigation pane and the grid pane to perform common functions more easily.

The following image and table depicts the toolbar buttons that appear at the top of the navigation pane.

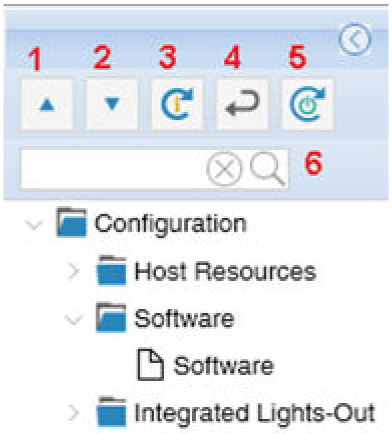


Figure 4: Toolbar buttons- navigation pane

Table 5: Toolbar buttons- navigation pane

Button	Name	Description
1	Collapse All	Collapse all folders by clicking it.
2	Expand All	Expand all folders by clicking it.
3	Refresh Status	Refreshes the device physical view.
4	Flip	Rotates the device view front and back.
5	AFO Appliance Reset	Restart the AFO appliance.
6	Search	When you type a partial or complete search string, the navigation pane changes to display only the entries associated with your search. To return to the full navigation pane display, click the x beside the **Search** dialog box.

Within **Configuration** folder, there are numerous sub-folders. To open a sub-folder, click the arrow to the left of the folder or double-click the folder to display the available tabs.

To close a folder, click the arrow once.

The following table describes the main folders available in the navigation pane.

Table 6: Navigation pane folders

Folder Name	Description
Configuration	Use configuration folder to open the following sub-folders: • Host Resources • Software • Integrated Lights-Out
Host Resources	Use Host Resources folder to gather details of the hosted services on the device.
Software	Use software folder to gather details of the software running and installed on the device.
Integrated Lights-Out	Use Integrated Lights-Out (iLO) folder to launch iLO and, to configure iLO IP address and SNMP settings.

Toolbar

The toolbar buttons provide quick access to commonly used operational commands. The buttons that appear vary depending on the tab you select. However, the Refresh, and Help buttons are on almost every screen.

The following list detail the toolbar buttons that appear at the top of the grid pane:

Table 7: Toolbar buttons- grid pane

Button	Name	Description
↻	Refresh	Use this button to refresh all data on the grid pane screen.
⏻	Shutdown Service	Use this button to shut down the selected service from the grid pane.
⏻	Start Service	Use this button to start the selected service. Click **Yes** in the confirmation window to start the service.
↻	Soft Reset	Use this button to restart a selected module. Click **Yes** in the confirmation window to restart a module.
⚙	Configure Network	Use this button to configure the network settings on the AFO appliance.

The following list detail some of the common toolbar buttons that appears on ADM:

Table 8: Common toolbar buttons

Button	Name	Description
✓	Apply	Execute all edits that you make.
⬚	Copy	Copy data from one or more fields ✱ **Note:** You can only copy and paste data in editable fields. The fields must have matching data type constraints.
📋	Paste	Paste the copied data to a new area within the same tab, a different tab or to another application. ✱ **Note:** You can paste data to an application outside your browser, such as a Microsoft Excel spreadsheet or Notepad. However, you cannot paste data from outside the ADM application to a field in the ADM application.
↶	Undo	Undo the last action.
⇨	Export	Exports device information displayed in Device pane grid in to a text file.
🖶	Print	Print the device information.
?	Help	Opens online Help for the current folder or tab.

Grid Pane

The Grid Pane is the main area on the right side of the window that displays each of the services (virtual machines) and the associated properties of the services. Use the Grid Pane to view or configure services on AFO appliance.

For more information, see the ADM Window on page 93 for the sample Grid Pane depicting the services configured on AFO appliance.

Monitoring Graphs

Located below the Grid pane to the right of the ADM Window on page 93, the Monitoring Graphs display the statistical view of the CPU usage and Memory usage of the services on the AFO device. The following table describes the graphs that appear at the bottom of the ADM window.

Table 9: Monitoring Graphs

Name	Description
Host Data	Displays the statistical view of the hosted data on the AFO server.
Service CPU Usage	Displays the CPU utilization of the services on the AFO device.
Service Memory Usage	Displays the memory utilization of the services on the AFO device.

ADM interface configuration

This section contains procedures for starting and using Appliance Device Manager (ADM). The software is built-in to the Avaya Fabric Orchestrator (AFO), and you do not need to install additional software.

Connecting to ADM when platform is up

Use this procedure to connect to ADM when AFO is up and running.

Before you begin

- Open one of the following browsers:
  - Mozilla Firefox, versions 40, 41
  - Microsoft Internet Explorer, versions 10, 11
- Ensure that AFO platform is running.
- Note the IP address of the AFO.

Procedure

1. In the address bar, enter the IP address of the system using the following formats: **`https://<IP_address>`** (default) or **`http://<IP_address>`**.

   Important:

   By default the web server is configured with the secure-only option, which requires you to use https to access ADM. To access ADM using http, you must disable the secure-only option.

2. Login to AFO using the Single Sign On (SSO):
    a. In the **User ID** field, type the user name. The default is admin.
    b. In the **Password** field, type the password. The default is admin123.
    c. Click **Log On**.

    The AFO menu bar is displayed.
3. On the AFO menu bar, click **Administration** > **Appliance Device Manager** .

    The system displays the Appliance Device Manager page.

Connecting to ADM when platform is down

Use this procedure to connect to ADM when AFO is down through the Management Server Console (MSC).

Before you begin

- Open one of the following browsers:
    - Mozilla Firefox, versions 40, 41
    - Microsoft Internet Explorer, versions 10, 11
- Ensure that AFO is down.

Procedure

1. In the address bar, enter the MSC server URL `https://<Fully Qualified Domain Name>`.

    Important:

    By default the web server is configured with the secure-only option, which requires you to use https to access ADM. To access ADM using http, you must disable the secure-only option.
2. Login to MSC using your login credentials:
    a. Enter `admin` as user name.
    b. Enter `Afo_123` as password. (default password).

    The AFO menu bar is displayed.
3. On the AFO menu bar, click **Administration** > **Appliance Device Manager** .

    The system displays the Appliance Device Manager page.

Using the configure network icon

About this task

Perform the following procedure to view or modify the existing network configuration of the AFO device.

Before you begin

- You must be logged in to AFO.

Procedure

1. From the AFO menu bar, click **Administration** > **Appliance Device Manager** .

   The system displays the Device Physical View window.

2. On the Device Physical View window, click ⚙ icon on the top-right corner of the Grid pane toolbar.

   The system displays **Configure Network** dialog-box.

3. On the **Network** and **FQDN and Credentials** section, view the existing information of the network configuration.

4. **(Optional)** To edit the existing network configuration information, modify the field values in the respective **Network** and **FQDN and Credentials** section.

   a. Enter the login password.

   b. Click **Update** to apply the changes.

Configure network icon field description

Use the data in the following table to use the **Configure network** icon.

Name	Description
IP Range	Specifies the list of IP addresses, that includes IP address of the server, services, and of the iLO.
Gateway	Specifies the default gateway address of the device.
Netmask	Specifies a 32-bit mask used to divide an IP address into subnets and specify the networks available hosts.
FQDN Prefix	Specifies prefix to a fully-qualified domain name. For example, in `afobeta2-monitoring.avaya.com`, *afobeta2* indicates the prefix.
FQDN Suffix	Specifies suffix to a fully-qualified domain name. For example, in `afobeta2-monitoring.avaya.com`, *avaya.com* indicates the suffix.
User Name	Specifies the user name. This field is read-only.
Password	Enter the login password.

Host Resources

Viewing the host resources- device information

Use this procedure to view the summary of the device information of the host resource.

Before you begin

- You must be logged into AFO.

Procedure

1. From the AFO menu bar, click **Administration** > **Appliance Device Manager**.

   The window displays the ADM window.
2. On the ADM window, select **Configuration** > **Host Resources** from the left navigation pane.
3. Click **Device** tab to view the device information.

   The Device tab displays on the right side of the ADM window.

Device tab field descriptions

Use the data in the following table to use the **Device** tab.

Name	Description
Index	Specifies a unique value for each logical storage area contained by the host.
Device Type	Specifies an indication of the type of device.
Description	Specifies the textual description of this device, including the device manufacturer and revision, and optionally, its serial number.
Status	Specifies the current operational state of the device.

A row of buttons at the top of the Device pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Viewing the host resources- processor information

Use this procedure to view the summary of the processor information of the host resource.

Before you begin

- You must be logged into AFO.

Procedure

1. From the AFO menu bar, click **Administration** > **Appliance Device Manager**.

   The system displays the ADM window.
2. On the ADM window, select **Configuration** > **Host Resources** from the left navigation pane.

3. Click **Processor** tab to view the processor information.

   The Processor tab displays on the right side of the ADM window.

Processor tab field descriptions

Use the data in the following table to use the **Processor** tab.

Name	Description
Index	Specifies a unique value for each logical storage area contained by the host.
Processor Load	Specifies processor utilization in percentage.

A row of buttons at the top of the Processor pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Viewing the host resources- network information

Use this procedure to view the summary of the device network information of the host resource.

Before you begin

- You must be logged into AFO.

Procedure

1. From the AFO menu bar, click **Administration** > **Appliance Device Manager**.

   The system displays the ADM window.

2. On the ADM window, select **Configuration** > **Host Resources** from the left navigation pane.
3. Click **Network** tab to view the device network information.

   The DeviceNetworkInfo tab displays on the right side of the ADM window.

Network tab field descriptions

Use the data in the following table to use the **Network** tab.

Name	Description
Index	Specifies a unique value for each logical storage area contained by the host.
Network Index	Specifies the value of ifIndex which corresponds to this network device.

A row of buttons at the top of the Network pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Viewing the physical storage information

Use this procedure to view the summary of the physical storage information of the hosted resources.

Before you begin

- You must be logged into AFO.

Procedure

1. From the AFO menu bar, click **Administration** > **Appliance Device Manager**.

   The system displays the ADM window.
2. On the ADM window, select **Configuration** > **Host Resources** from the left navigation pane.
3. Click **Storage**.

   The **Physical** and **Logical** sub-tabs displays on the right side of the ADM window.
4. Select **Physical** sub-tab to view physical storage information of the hosted resources.

Physical storage tab field descriptions

Use the data in the following table to use the **Physical** tab.

Name	Description
Index	Specifies a unique value for each device contained by the host.
Access	Specifies the privileges that determines the operations that you can perform on device.
Media	Specifies an indication of the type of media used in this long- term storage device.
Removable	Specifies whether or not the disk media may be removed from the drive.
Capacity (GB)	Specifies the total size for this long-term storage device.

A row of buttons at the top of the Physical pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Viewing the logical storage information

Use this procedure to view the summary of the logical storage information of the hosted resources.

Before you begin

- You must be logged into AFO.

Procedure

1. From the AFO menu bar, click **Administration** > **Appliance Device Manager**.

   The system displays the ADM window.
2. On the ADM window, select **Configuration** > **Host Resources** from the left navigation pane.
3. Click **Storage**.

   The Physical and Logical sub-tabs displays on the right side of the ADM window.
4. Select **Logical** sub-tab to view logical storage information of the hosted resources.

Logical storage tab field descriptions

Use the data in the following table to use the **Logical** tab.

Name	Description
Index	Specifies a unique value for each logical storage area contained by the host.
Type	Specifies the type of storage represented by this entry.
Description	Specifies a description of the type and instance of the storage described by this entry.
Allocation Units (Bytes)	Specifies the size, in bytes, of the data objects allocated.
Size (GB)	Specifies the size of the storage represented by this entry, in units of hrStorageAllocationUnits.
Used (GB)	Specifies the amount of the storage represented by this entry that is allocated, in units of hrStorageAllocationUnits.

A row of buttons at the top of the Logical pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Viewing the host resources- partition information

Use this procedure to view the partition details of the host resources in gigabyte (GB).

Before you begin

- You must be logged into AFO

Procedure

1. From the AFO menu bar, click **Administration** > **Appliance Device Manager**.

   The system displays the ADM window.
2. On the ADM window, select **Configuration** > **Host Resources** from the left navigation pane.
3. Click **Partition**.

   The Partition sub-tab displays on the right side of the ADM window.

Partition tab field descriptions

Use the data in the following table to use the **Partition** tab.

Name	Description
Index	Specifies a unique value for each logical storage area contained by the host.
Label	Specifies a textual description of this partition.

Table continues…

Name	Description
ID	Specifies a descriptor which uniquely represents this partition to the responsible operating system.
Size (GB)	Specifies the size of this partition in gigabyte (GB).
IfIndex	Specifies the index of the file system mounted on this partition in gigabyte (GB).

A row of buttons at the top of the Partition pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Viewing the host resources- file system

Use this procedure to view the file system details of the host resources.

Before you begin

- You must be logged into AFO

Procedure

1. From the AFO menu bar, click **Administration** > **Appliance Device Manager**.

   The system displays the ADM window.

2. On the ADM window, select **Configuration** > **Host Resources** from the left navigation pane.
3. Click **File System**.

   The File system sub-tab displays on the right side of the ADM window.

File system tab field descriptions

Use the data in the following table to use the **File Sytem** tab.

Name	Description
Index	Specifies a unique value for each file system local to this host.
Mount Point	Specifies a directory (typically an empty one) in the currently accessible file system on which an additional file system is mounted.
Type	Specifies the type of the file system.
Access	Specifies the privileges that determines the operations that you can perform on device.
Bootable	Specifies if the file system contains special files required to boot into an system.
StorageIndex	Specifies a summary of the data distribution on the disk and provides an additional method to eliminate unnecessary disk Input and output (I/O).

Table continues…

Name	Description
LastFullBackupDate	Specifies the last backup date when the complete file system was copied to another storage device for backup.
LastPartialBackupDate	Specifies the last partial backup date when a portion of this file system was copied to another storage device for backup.

A row of buttons at the top of the File System pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Viewing host resources- system information

Use this procedure to view the system information of the host resources.

Before you begin

- You must be logged into AFO

Procedure

1. From the AFO menu bar, click **Administration** > **Appliance Device Manager**.

   The system displays the ADM window.

2. On the ADM window, select **Configuration** > **Host Resources** from the left navigation pane.
3. Click **System**.

   The System sub-tab displays on the right side of the ADM window.

System tab field descriptions

Use the data in the following table to use the **System** tab.

Name	Description
Processes	Specifies the number of process contexts currently loaded or running on this system.
Initial Load Device	Specifies the device index from which this host is configured to load its initial operating system configuration.
Num Users	Specifies the number of users sessions for which this host is storing state information.
Max Processes	Specifies the maximum number of process contexts this system can support.
Up Time	Specifies the time during which a system is operational.
System Date	Specifies the host local date and time of the day.

A row of buttons at the top of the System pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Software

Viewing the software execution information

Use this procedure to view the status of the software execution.

Before you begin

- You must be logged into AFO.

Procedure

1. From the AFO menu bar, click **Administration** > **Appliance Device Manager**.

   The system displays the ADM window.

2. On the ADM window, select **Configuration** > **Software** from the left navigation pane.
3. Click **Software**.

   The SoftwareRunning and SoftwareInstalled sub-tab displays on the right side of the ADM window.

4. Click **SoftwareRunning** tab.

Software execution tab field descriptions

Use the data in the following table to use the **SoftwareRunning** tab.

Name	Description
Run Index	Specifies a unique value for each piece of software running on the host.
Run Name	Specifies a textual description of this running piece of software, including the manufacturer, revision, and the name by which it is commonly known.
Run Path	Specifies a description of the location for long-term storage (e.g. a disk drive).
Run Parameters	Specifies the parameters supplied to this software .
Run Status	Specifies the software execution status.

A row of buttons at the top of the Software Running pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Viewing the software installed information

Use this procedure to view the software installed information.

Before you begin

- You must be logged into AFO.

Procedure

1. From the AFO menu bar, click **Administration** > **Appliance Device Manager**.

   The system displays the ADM window.

2. On the ADM window, select **Configuration** > **Software** from the left navigation pane.
3. Click **Software**.

   The SoftwareRunning and SoftwareInstalled sub-tab displays on the right side of the ADM window.

4. Click **SoftwareInstalled** tab.

Software installed field descriptions

Use the data in the following table to use the **SoftwareInstalled** tab.

Name	Description
Index	Specifies a unique value for each piece of software installed on the host.
Name	Specifies a textual description of the installed piece of software, including the manufacturer, revision, the name, and optionally, its serial number.
Type	Specifies the software type.
Date	Specifies the last-modification date of this application.

A row of buttons at the top of the Software Installed pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Integrated Lights-Out

Launch iLO

Use this procedure to launch iLO.

Before you begin

- You must be logged into AFO.

Procedure

1. From the AFO menu bar, click **Administration** > **Appliance Device Manager**.

   The system displays the ADM window.

2. On the ADM window, select **Configuration** > **Integrated Lights-Out** from the left navigation pane.
3. To launch iLO, click **Launch iLO**.

   The system launches the HP iLO 4 web interface in a separate window.

Viewing the iLO- overview information

Use this procedure to view the overview information of the iLO.

Before you begin

- You must be logged into AFO.

Procedure

1. From the AFO menu bar, click **Administration** > **Appliance Device Manager**.

   The system displays the ADM window.
2. On the ADM window, select **Configuration** > **Integrated Lights-Out** from the left navigation pane.
3. Click **Overview** tab to view the overview information of the iLO.

   The Overview tab displays on the right side of the ADM window.

Overview tab field descriptions

Use the data in the following table to use the **Overview** tab.

Name	Description
System ROM	Specifies the system ROM version information for the redundant ROM image.
Server Serial Number	Specifies the serial number of the physical system unit. This field is empty if the system does not report the serial number function.
Product ID	Specifies the product ID of the system unit. This field is empty if the system does not report the product ID.
Product Name	Specifies the appliance product name.
Backup System ROM	Specifies the system ROM version information for the redundant ROM image.
Product Service No	Specifies the service number of the system unit.
iLO Hostname	Specifies iLO serial number.
iLO Firmware Version	Specifies the revision of the firmware on the iLO.
UUID	Specifies the globally unique identifier in canonical format of this physical server.

Table continues…

Name	Description
	If the OS cannot determine a unique ID, it displays the default variable as blank.
Server Power	Specifies the current power state for the server. The power cap reaches state indicates there was an attempt to power on, but the server could not reserve enough power.

A row of buttons at the top of the Overview pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Viewing the iLO- system information

Use this procedure to view the iLO system information to monitor server hardware health.

Before you begin

- You must be logged into AFO.

Procedure

1. From the AFO menu bar, click **Administration** > **Appliance Device Manager**.

   The system displays the ADM window.

2. On the ADM window, select **Configuration** > **Integrated Lights-Out** from the left navigation pane.

3. Click **System Information** tab to view the overview information of the iLO.

   The System Information tab displays the following sub-tabs on the right side of the ADM window:

   - Fan
   - Temperature
   - Power
   - Memory
   - Processor
   - Firmware

Viewing the system- fan information

Use the data in the following table to use the iLO system **fan** tab.

Name	Description
Fan	Specifies the fan list in ascending serial number.
Location	Specifies the location of the fan in the system..
Status	Specifies the condition of the fan.

Table continues…

Name	Description
Speed	Specifies the speed of the fan. This field value is set if the fan type is `tachOutput`.
Fan Present	Specifies the described fan availability in the system as: • absent • present
Type	Specifies the fan type.
Fan Redundant	Specifies if the fan is in a redundant configuration, to monitor the system health.

A row of buttons at the top of the pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Viewing the system- power information

Use the data in the following table to use the iLO system **Power** tab.

Name	Description
Bay	Specifies the bay number to index within this chassis.
Model	Specifies the power supply model number.
Serial	Specifies the serial number of the model.
Hot Plug	Specifies if the power supply is capable of being removed or inserted while the system is in an operational state. Specifies the value as `True` or `False`.
Firmware	Specifies the power supply firmware revision.
Spare	Specifies the spare part number.
Status	Specifies the power status.
Present Power Reading	Specifies the power reading in Watts.
Present	Specifies the currently used capacity of the power supply in Watts.
Redundant	Specifies the redundancy state of the power supply.

A row of buttons at the top of the pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Viewing the system-temperature information

Use the data in the following table to use the iLO system **Temperature** tab.

Name	Description
Index	Specifies a temperature sensor entry.
Location	Specifies the location of the temperature sensor present in the system.
Reading	Specifies the current temperature sensor reading in degrees Celsius. The default value is `-99`.
Threshold	Specifies the type of temperature sensor.
Status	Specifies the temperature sensor condition.

A row of buttons at the top of the pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Viewing the system-memory information

Use the data in the following table to use the iLO system **Memory** tab.

Name	Description
Module	Specifies the unique memory DIMM on memory board or cartridge.
Memory Location	Specifies a text description of the hardware location, on complex multi SBB hardware only, for the memory module. A `NULL` field value indicates that the hardware location could not be determined or is irrelevant.
Status	Specifies the current status of the correctable memory errors for this memory module.
HP Smart Memory	Specifies whether the DIMM slot is populated with an HP smart memory DIMM.
Part Number	Specifies the part number.
Type	Specifies the type of memory module installed.
Size (GB)	Specifies the memory size in GB.
Maximum Frequency	Specifies the memory module maximum frequency in MHz. The default value is `Zero`.
Minimum Voltage	Specifies the minimum voltage needed for the module to operate, in millivolts.
Technology	Specifies the technology type of memory module installed.

A row of buttons at the top of the pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Viewing the system-processor information

Use the data in the following table to use the iLO system **Processor** tab.

Name	Description
Index	Specifies a unique and auto-generated index number.
Processor Name	Specifies the processor name.
Processor Status	Specifies the processor status.
Processor Speed	Specifies the processor speed in MHz.
Execution Technology	Specifies the number of cores in this CPU module. The default value is `Zero`.
Power Status	Specifies the power status of the processor.

A row of buttons at the top of the pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Viewing the system-firmware information

Use the data in the following table to use the iLO system **Firmware** tab.

Name	Description
Index	Specifies a firmware version index. The firmware version index uniquely identifies an entry in the cpqHoFwVer table.
Display Name	Specifies the firmware version device display name. It indicates the display name of the device containing the firmware.
Version	Specifies the version of the device firmware.

A row of buttons at the top of the pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Viewing the iLO- network information

Use this procedure to view the iLO network information to monitor server hardware health.

Before you begin

- You must be logged into AFO.

Procedure

1. From the AFO menu bar, click **Administration** > **Appliance Device Manager** .

   The system displays the ADM window.
2. On the ADM window, select **Configuration** > **Integrated Lights-Out** from the left navigation pane.
3. Click **Network Information** tab to view the network information.

The Network tab displays on the right side of the ADM window.

iLO network tab field descriptions

Use the data in the following table to use the iLO **Network** tab.

Name	Description
Device Model	Specifies the iLO network interface controller model.
Location	Specifies the location of the network interface controller associated with the iLO.
Type	Specifies the Integrated Lights-Out network interface controller type.
MAC Address	Specifies the MAC address of the Integrated Lights-Out network interface controller.
Condition	Specifies the condition of the network. This represents the overall condition of the Integrated Lights-Out network interface controller (NIC).
Status	Specifies the Integrated Lights-Out network interface controller (NIC) enabled status.
DhcpUse	Specifies the Dynamic Host Configuration Protocol (DHCP) status as `enabled` or `disabled`.

A row of buttons at the top of the pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Viewing the iLO- logs information

Use this procedure to view the logs information to monitor server hardware health.

Before you begin

- You must be logged into AFO.

Procedure

1. From the AFO menu bar, click **Administration** > **Appliance Device Manager** .

   The system displays the ADM window.

2. On the ADM window, select **Configuration** > **Integrated Lights-Out** from the left navigation pane.
3. Click **Logs** tab to view the log information.

   The Integrated Management Log and iLO Event Log sub-tabs displays on the right side of the ADM window.

Integrated management log field descriptions

Use the data in the following table to use the **Integrated Management Log** tab.

Name	Description
ID	Specifies a table of system event log entries.
Severity	Specifies a number that uniquely specifies this system event log severity.
Class	Specifies the iLO event log entry class designation.
LogEntryCode	Specifies the event log entry code designation as defined in **Class** field.
Count	Specifies the event log entry occurrence count. This field represents the number of times this event has occurred starting from the initial time until the last modified time.
Initial Update	Specifies the time stamp when the event log entry was first created.
Last Update	Specifies the time stamp when the event log entry was last modified.
Description	Specifies a text description of the event log entry.

A row of buttons at the top of the pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

iLO event log tab field descriptions

Use the data in the following table to use the **iLO Event Log** tab.

Name	Description
No	Specifies an index that uniquely specifies this entry.
id	Specifies a number assigned by the iLO firmware.
Initial Update	Specifies the time and date for this event log entry.
Description	Specifies a text description of the event log entry.

A row of buttons at the top of the pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Viewing the iLO- thermal information

Use this procedure to view the thermal information to monitor server hardware health.

Before you begin

- You must be logged into AFO.

Procedure

1. From the AFO menu bar, click **Administration** > **Appliance Device Manager**.

   The system displays the ADM window.

2. On the ADM window, select **Configuration** > **Integrated Lights-Out** from the left navigation pane.

3. Click **Thermal** tab to view the thermal information.

   The Thermal tab displays on the right side of the ADM window.

Thermal field descriptions

Use the data in the following table to use the **Thermal** tab.

Name	Description
Condition	Specifies the overall condition of the system thermal environment. The value will be `ok` if ThermalTempStatus, ThermalSystemFanStatus, and ThermalCpuFanStatus are all okay.
Temperature Status	Specifies the status of the system temperature sensors.
System Fan Status	Specifies if the system fans are operating properly.
CPU Fan Status	Specifies if the CPU fans are operating properly.

A row of buttons at the top of the pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Viewing the iLO- CPU information

Use this procedure to view the CPU information to monitor server hardware health.

Before you begin

- You must be logged into AFO.

Procedure

1. From the AFO menu bar, click **Administration** > **Appliance Device Manager**.

   The system displays the ADM window.

2. On the ADM window, select **Configuration** > **Integrated Lights-Out** from the left navigation pane.
3. Click **CPU** tab to view the CPU information.

   The CPU tab displays on the right side of the ADM window.

CPU tab field descriptions

Use the data in the following table to use the **CPU** tab.

Name	Description
Bay	Specifies the physical drive bay Location.
Status	Specifies the physical drive status.
Condition	Specifies the condition of the device.
Model	Specifies a text description of the physical drive. The text that appears depends upon who manufactured

Table continues…

Name	Description
	the drive and the drive type. If a drive fails, note the model to identify the type of drive necessary for replacement.
Revision	Specifies the revision number of the model.
Drive Location	Specifies the drive location.
Size	Specifies the size of the physical drive in megabytes. This field is only applicable for controllers which support SCSI drives.
SerialNo	Specifies the serial number of the CPU.
SmartStatus	Specifies the physical drive S.M.A.R.T status.
ConfigStatus	Specifies the configuration status.
RationalSpeed	Specifies the drive array physical drive rotational speed.
DriverType	Specifies the driver type.
SataVersion	Specifies the physical drive SATA version.
HostConnector	Specifies the host connector information to which the drive is ultimately attached.
Connector	Specifies to which box instance this physical drive belongs. A value of -1 is returned for drives that do not support cpqDaPhyDrvBoxOnConnector.
Location	Specifies the location of the drive in relation to the controller.
LinkRate	Specifies the drive array physical drive negotiated link rate.
DriveSupport	Specifies the drive array physical drive native command queueing.
MultiPath	Specifies the drive array physical drive multi-path access status.
MediaType	Specifies the drive array physical drive media type.
CurrentTemperature	Specifies the current temperature in Celsius.
Threshold	Specifies the threshold temperature value.
Max Temperature	Specifies the maximum temperature in Celsius.
SSDWearStatus	Specifies the SSD status.
AuthenticationStatus	Specifies the authentication status as `passed` or `failed`.

A row of buttons at the top of the pane provides a quick method to perform common functions. For more information on list and description of buttons, see Navigation Pane on page 94.

Chapter 11: Software upgrade and patching support for AFO

Overview

Upgrading is the process of updating the existing managed elements software version with a new version. In Avaya Fabric Orchestrator (AFO), the managed elements include; the virtual machine, applications for all the elements, and devices that are managed by AFO.

Software Patch (Update or Feature Pack) is an incremental change to the major release in terms of new features and bug fixes. The process of applying this patch is software patching.

The Solution Software Director (SSD) checks the compatibility of the available software with the AFO managed elements and recommends the required upgrades and updates based on your entitlements.

Solution Software Director (SSD)

You can perform software upgrade and patching using SSD through the AFO web interface. On the menu bar, click **Administration** > **Solution Software Director** to perform a software upgrade. You can upgrade AFO using any one of the following two methods depending on the scenarios as defined in the table below:

- Easy mode upgrade
- Advanced mode upgrade

The following table lists different scenarios and type of upgrades:

Table 10: Type of Upgrades

Scenario	Type of Upgrade
When Platform VM is up	You can perform either Easy mode upgrade or Advanced mode upgrade
When Platform VM is down	You can perform either Easy mode upgrade or Advanced mode upgrade
When PLDS is not accessible from server (PLDS connectivity status is offline)	You can only perform Advanced mode upgrade
When PLDS is accessible from server ((PLDS connectivity status is online)	You can perform either Easy mode upgrade or Advanced mode upgrade

Table continues…

Scenario	Type of Upgrade
Using SSD for MSC self-upgrade in an AFO deployment	You can perform a self-upgrade of MSC from SSD. This means the service running the upgrade software upgrades itself.

Logging in to SSD when platform service is down

About this task

You can perform this task when you cannot access the AFO system to perform software upgrades as the platform or monitoring services that handle authorization or the user interface of the Solution Software Director is down. In this scenarios, the local login feature of SSD takes over and redirects you to the local login screen of the deployment. You need to use machine user name and password to get access to the AFO system.

Before you begin

- Login to SSD through the MSC server URL `https://<Fully Qualified Domain Name>/SSD`.
- Enter MSC user name and password to access this platform.

  ✱ **Note:**

  You can enter default user name and password as `admin/Afo_123` to login.

Procedure

1. On the menu bar, click **Administration** > **Solution Software Director**.

   The system displays the **Solution Software Director** page.

2. Click **Perform Upgrade in Advanced Mode** or **Perform Upgrade in Easy Mode** depending on the AFO system connectivity with the PLDS server.

   For more information on how to perform Advanced mode upgrade, see Advanced mode upgrade when PLDS connectivity status is online on page 120 and Advanced mode upgrade when PLDS connectivity status is offline on page 121.

Easy mode upgrade

Avaya Solution Software Director (SSD) runs on the Management Server Console (MSC) virtual machine of the AFO and is only accessible for authorized users of AFO. For Easy mode upgrade, SSD automatically downloads the required software bundles from PLDS and applies them to your system.

✱ **Note:**

Easy mode upgrade is not available if your PLDS connectivity status is offline.

About this task

You can perform the Easy mode upgrade when the PLDS connectivity status is online.

Procedure

1. Login to AFO using the administrator credentials.

   The AFO home page is displayed.

2. On the menu bar, click **Administration** > **Solution Software Director**.

   The system displays the SSD page.

3. On the SSD page, click **Perform Upgrade in Easy Mode**.

   The system displays the End User License Agreement window.

4. Accept the end user license agreement certificate.

   The system displays the **Easy Mode** page.

5. On the **Easy Mode** page:

   - Click **Analysis**. The system automatically starts performing analysis to find releases and choose the recommended release for an upgrade.
   - Click **Download**. The system automatically downloads the required bundles for upgrade from the Avaya PLDS site.
   - Click **Pre-Checks**. The system performs prerequisite checks of the bundle.
     - Upgrade button is enabled only after successful completion of the pre-checks.
     - If any of the service pre-checks fail, the upgrade is blocked from execution. You must see the Activity log section to rectify the problem before you perform an upgrade.

       Note:

       The **Activity Logs** section provide runtime updates of the upgrade activities to all logged in users of the AFO SSD at that point in time.

6. On the **Easy Mode** page, click **Upgrade** to proceed with the upgrade. Upgrade button is enabled only after successful completion of the pre-checks.

   Note:

   Once an Easy mode upgrade is complete, on attempting to retry an upgrade, the **Analysis** section provides a message that the system is up-to-date and disables the rest of the options, thereby preventing further upgrades.

Advanced mode upgrade

Avaya Solution Software Director (SSD) runs on the Management Server Console (MSC) virtual machine of the AFO and only accessible for authorized users of AFO.

- You can perform the Advanced mode upgrade using the platform service by logging into AFO using administrator credentials.
- On the AFO menu bar, click **Administrator** > **Solution Software director**.

When the platform service is down and you cannot access the AFO web-interface, see Logging in to SSD when platform service is down on page 118.

Unlike the Easy mode upgrade, you can perform the Advanced mode upgrade even when the PLDS connectivity status is offline.

Advanced mode upgrade when PLDS connectivity status is online

About this task

Perform this task to upgrade the system when the PLDS connectivity status is online and PLDS is accessible from the server.

Before you begin

- Ensure that you are logged on to Avaya Solution Software Director (SSD).
- Verify that the **PLDS Connectivity Status** on the SSD page is Online.

  Note:

  If the **PLDS Connectivity Status** is Offline, see Advanced mode upgrade when PLDS connectivity status is offline on page 121.

Procedure

1. Click **Perform Upgrade in Advanced mode**.

   The system displays the **Inventory** page. The **Inventory** page displays the list of service: **Name, IP address, Type, and Version**.
2. On the **Inventory** page, click **Analysis** to analyze and retrieve the latest available releases that can be upgraded.

   The system displays the **Analysis** page. The **Analysis** page displays the latest available releases based on the analysis in the **Release** drop-down column.
3. On the **Analysis** page, select the **Release**.

   The color code near the **Name** column is displayed.

   The following table provides the list of color codes and their significance:

Table 11: Color-Code significance

Color Code	Description
Green	No new upgrade or update is available. The system is already up-to-date.
Red	Compatible upgrade or update is available on PLDS but not available in the **Software Library**.
Yellow	Compatible upgrade or update is available in the **Software Library** (both online and offline mode).
Purple	Compatible upgrade or update is available on PLDS. However, you are not entitled to an upgrade.
Grey	Analysis has not been run. Perform **Analysis**.

4. Click **Download Bundle**. The system automatically downloads the bundles required for the upgrade from the PLDS.
5. Click **Precheck** to perform the prerequisite check of the downloaded bundles.

   The **Precheck** page displays the result on a per service basis as `Pass` or `Fail` along with the description.

   Note:

   If any of the service pre-checks fail, the upgrade is blocked from the execution. See the Activity logs section to rectify the problem and perform the upgrade.

   Tip:

   Activity Logs provide runtime updates of the upgrade activities to all logged in users of the AFO SSD at that point in time.
6. On the **Precheck** page, click **Upgrade** after successful completion of the pre-check to upgrade the system.

   The **Upgrade** page displays the status of the upgrade. The **Progress** column displays a green color bar when the upgrade is complete.

Advanced mode upgrade when PLDS connectivity status is offline

About this task

Perform this task when PLDS connectivity status is offline and PLDS is not accessible from the server.

Before you begin

- Ensure that you are logged on to Avaya Solution Software Director (SSD).
- Verify that **PLDS Connectivity Status** on the SSD page is *Offline*.

Important:

Based on the availability of PLDS access from the server, the PLDS connectivity status shows as online or offline.

Procedure

1. Click **Perform Upgrade in Advanced mode**.

   The system displays the **Inventory** page. The **Inventory** page displays the list of service: **Name, IP address, Type, and Version**.

2. On the **Inventory** page, click **Upload Matrix** to get updated recommendation for upgrades.

   The system displays the End User License Agreement window.

3. Select **I Agree the terms of License Agreement** and click **OK** to agree the license agreement to upload files pertaining to Avaya AFO upgrades.

4. On the **Upload Compatibility Matrix** page, click **Browse** to upload compatibility matrix from the system.

   If the latest compatibility matrix is unavailable on the system, download the latest compatibility matrix in the software library from the Avaya Support Site when PLDS server is online.

5. Click **Upload**. The system displays a `success` or a `failure` message for the file uploaded.

   Note:

   If a failure error message displays, see **Activity Logs** to rectify the problem and perform the upgrade.

   Tip:

   Activity Logs provide runtime updates of the upgrade activities to all logged in users of the AFO SSD at that point in time.

6. Click **Analysis** after successful completion of the upload. The **Analysis** page displays the latest available releases based on the analysis in the **Release** drop-down column.

   The system performs the analysis to retrieve the latest available releases for the upgrade.

7. On the **Analysis** page, select the **Release**.

   The color-code near the **Name** column is displayed. For more information on significance of a color code, see table Color-Code significance on page 121.

8. Click **Upload Bundle**. The **Upload Bundle** page displays the bundles required for the upgrade along with their availability.

   Choose from the following two options to complete uploading a bundle:

Choice Option	Choice Description
If the requisite bundles are already available in the Software Library	**Browse** column is disabled and **Progress** column displays a status as **File is available**.

Choice Option	Choice Description
If the requisite bundles are not available in the Software Library	Click **Browse** to upload the bundle and click **Start Upload**.

9. Click **Precheck** to perform the prerequisite check of the downloaded bundles.

   The **Precheck** page displays the result on a per service basis as `Pass` or `Fail` along with the description.

   ✱ **Note:**

   If any of the service pre-checks fail, the upgrade is blocked from the execution.

   See **Description** column and **Activity Logs** section for more information. You must rectify the issue to perform an upgrade.

10. On the **Precheck** page, click **Upgrade** after successful completion of the pre-check to upgrade the system.

Chapter 12: Logging and Log Harvesting

Understanding Logging

Avaya Fabric Orchestrator (AFO) offers Common Logging Framework for Audit, Operation, and Security Log messages of applications in the current release.

Overview

Logging is a set of serviceability feature. AFO Logging feature allows you to identify, understand system status, analyze, and resolve problems quickly through a consolidated view of different applications.

The following table describes the type of logs that are generated as part of AFO:

Table 12: AFO Log Type

Log Type	Description
Audit Log	Use Audit Log for regulatory compliance and customer agreements. Audit Logs provides an Audit Trail of all the changes and activities performed in the system.
Operational Log	Use Operational Log for tracking and recording all operational activities in AFO.
Syslog	Use Syslog for system related logs and for syslog listeners outside the system.
Security Log	Use Security Log for tracking and recording administration, access and security related activities in AFO.

Avaya Common Logging Format (CLF)

Avaya Common Logging Format (CLF) is a standard logging format in Avaya. AFO uses Avaya CLF for consistent implementation of logging and events across Avaya network devices, systems, and applications.

AFO generates a unique Log ID for every Audit Log and Operational Log message.

Understanding Log Harvesting

Log Harvesting

Log Harvesting is a process of backing up the log files for historical purpose. This process involves; keeping older log files in a separate directory, providing facility to upload to-be-purged log files to a external server (before purging).

Log Harvesting supports retrieval, archival and analysis of required log files from multiple hosts. Log Harvesting runs automatically, and you can specify an external server to save the purged files using the MSC preferences. For more information, see About MSC Preferences on page 61.

You can perform Log Purging at scheduled interval or on-demand basis. In both the scenarios, Log Harvesting collects all the required logs available on the AFO virtual machine, archives them, and stores them at a separate location. If, Log Harvesting requires a file from different host, you must specify the details of the required log files and the host machine address.

Important:

You can perform Log Harvesting for only Operational Log, Audit Log, and Security Log.

External Syslog Server

AFO provides *External Syslog server* as a standard interface to collect and display the harvested logs.

The External Syslog server displays a list of logs where you can view the details of each log, perform a search for logs, and filter specific logs. The log details include information about the event that generates the log, the severity level of the log, and other relevant information. You can search logs based on search conditions and set filters to view logs that match the filter criteria.

You can upload the harvested logs automatically to an external syslog server using the standard protocols, such as FTP, SCP/SFTP through AFO Preference.

For more information on configuring the preferences settings related to the Logging, and Log Harvesting tasks, see Managing Preferences on page 45.

One Click Log Collection (OCLC) for AFO

Avaya Fabric Orchestrator (AFO) allows you to run a single command to collect all applications logs (debug/trace/operational/audit/security) into a single archive, for all issues related to troubleshooting. Use this information to perform One Click Log Collection for applications logs generated on the centralized server on demand in a single click.

Overview

- The One click log collection feature is developed by extending the existing **`createLogArchive.sh`** command which collects log files and other required configurations from individual applications.
- The command gets executed remotely from Management Server Console (MSC) on every applicable system and collects the archive to a central place.

Related links

One Click Log Collection configuration using CLI on page 126

One Click Log Collection configuration using CLI

About this task

Use this procedure to perform One Click Log Collection on a centralized server in a single click. This procedure will help you to collect logs into a single archive from all the applications deployed on AFO.

Before you begin

- Ensure that you are logged on to the Management Server Console (MSC) server.
- Enter `root user name` and `password`.

Procedure

1. Run the following command on MSC server to collect logs:

   ```
   /opt/avaya/afo/infra/OneClickLogCollect.sh
   ```

2. The collected logs are compressed into a single archive and stored in the directory.

   The filename of the generated archive is displayed on the system.

   Note:

   Each time you run the command, the system generates a new zip file at the same location.

Related links

One Click Log Collection (OCLC) for AFO on page 125

Chapter 13: Licensing overview

Licensing in AFO uses a Web-based License Manager (WebLM) to manage licenses. WebLM is a Web-based license manager that facilitates easy tracking of licenses. To track and manage licenses in an organization, WebLM requires a license file from the Avaya Product Licensing and Delivery System (PLDS) Web site at http://plds.avaya.com.

The license file of a software product is in an XML format. The license file contains information regarding the product, the major release, the licensed features of the product, and the licensed capacities of each feature that you purchase. After you purchase a licensed Avaya software product, you must activate the license file for the product in PLDS and install the license file on the WebLM server.

License activations in PLDS require the HostID of the WebLM server and Monitoring VM HostID for inclusion in the license file. The HostID of the WebLM server is displayed on the Server Properties page of the WebLM.

For more information on how to generate HostID, see CLI commands for AFO on page 22.

Obtaining the license file

About this task

Obtain a license file from PLDS to install on the WebLM server for each licensed Avaya product that you require to manage from the WebLM server. For additional information on using PLDS, *Getting Started with Avaya PLDS for Avaya Networking Products*, NN46199-300. All licensing activities are performed through the Avaya PLDS Portal at http://plds.avaya.com.

⚠ **Caution:**

Do not modify the license file that you receive from Avaya. WebLM does not accept a modified license file.

Before you begin

You need the host ID of the WebLM server and Monitoring VM to obtain the license file from PLDS. To generate the host ID, use the **`afo-hostid`** command. For more information, see AFO Command Line Interface on page 22.

Procedure

1. Log on to the AFO.

2. On the AFO menu bar, click **Administration** > **Licenses**.

   The WebLM Home page displays.

3. In the left navigation pane, click **Server properties**.

   Server Properties displays on the right navigation pane.

4. Note the **Primary Host ID.**

   Displays the Host ID for this instance of the WebLM server. Use this for generating and installing licenses on this instance of the WebLM server.

5. Using the host ID, generate the license from PLDS.

Installing a license file

About this task

Perform this procedure to install a license to an application.

Before you begin

- Obtain the license file from the Avaya Product Licensing and Delivery System (PLDS) website at http://plds.avaya.com.
- Ensure that you are logged on to AFO as an administrator.

Procedure

1. On the AFO menu bar, click **Administration** > **Licenses**.

   The system displays the WebLM Home page.

2. In the left navigation pane, click **Install License**.

   The system displays the Install License page.

3. On the Install license page, enter the license file path in the **Enter license path** field. You can also click **Browse** to select the license file.

4. Click **Install** to install the license file.

   WebLM displays a message upon successful installation of the license file. The installation of the license file can fail for various reasons, such as:

   - WebLM finds an invalid digital signature on the license file. If you get such an error, request PLDS to redeliver the license file.
   - The current capacity use exceeds the capacity in the installed license.

Exporting a license file

About this task

Perform this procedure to export a license from the product name table to the local machine. Selection of one license file from an application exports all licenses for that application.

Before you begin

Ensure that you are logged on to AFO as an administrator.

Procedure

1. On the AFO menu bar, click **Administration** > **Licenses**.

   The system displays the WebLM Home page.

2. In the product name table, select the product license to be exported.
3. Click **Export All Licenses**.
4. License file download message with the file path name displays on top of the **WebLM Home** page.

Viewing the license capacity and utilization of the product features

About this task

Use this procedure to view the license capacity and license utilization of a product for which the license capacity and license utilization of a product for which you installed a license file.

Before you begin

- Log on to the AFO.
- Install the license file on the WebLM server for the licensed product.

the

Procedure

1. On the AFO menu bar, click **Administration** > **Licenses**.

   The system displays the WebLM Home page.

2. In the left navigation pane, click **Licensed products** and select the product name.

   The system displays the **Installed License Files** table in the right navigation pane.

3. Click the **WebLM Host ID- Client Host ID** hyperlink to view the license capacity of the license file for the selected host ID.

   The system also displays the element display name, element ID, and license file host IDs for the element.

Viewing the server properties

Before you begin

Ensure that you are logged on to AFO.

Procedure

1. On the AFO menu bar, click **Administration** > **Licenses**.

   The system displays the WebLM Home page.

2. In the left navigation pane, click **Server properties**

   ✱ **Note:**

   The host ID specified in PLDS is embedded in the license file. You can install the license file only if the host ID of the server that hosts WebLM and Monitoring VM matches the host ID in the license file. Therefore, when you request for a license file, specify the correct host ID of the server that hosts WebLM and host ID of the Monitoring VM.

Uninstalling a license file

About this task

Use this procedure to uninstall a license file.

Procedure

1. On the AFO menu bar, click **Administration** > **Licenses**.

   The system displays the WebLM Home page.

2. In the left navigation pane, click **Uninstall License**.
3. On the Uninstall License page, select the license file that you want to uninstall.
4. Click **Uninstall**.

   If the license file you selected cannot be uninstalled, the system displays only the **Cancel** button.

Chapter 14: Troubleshooting

This chapter provides the diagnostic and troubleshooting utilities information to isolate problems in your Avaya Fabric Orchestrator (AFO) current release.

AFO Service

The AFO Service utility allows you to easily stop, start, or restart the application service for any particular or multiple virtual machines without hindering your current application service. The options available for AFO Service utility are:

1. Help Command
2. Command to start, stop, or restart the application service on a particular virtual machine
3. Command to start, stop, or restart the application service on multiple virtual machines
4. Command to start, stop, or restart the application service on all the virtual machines

Condition

On AFO multiple services runs on different virtual machines. There may be incidents where you want to start, stop, or restart the application service for any particular or multiple virtual machines.

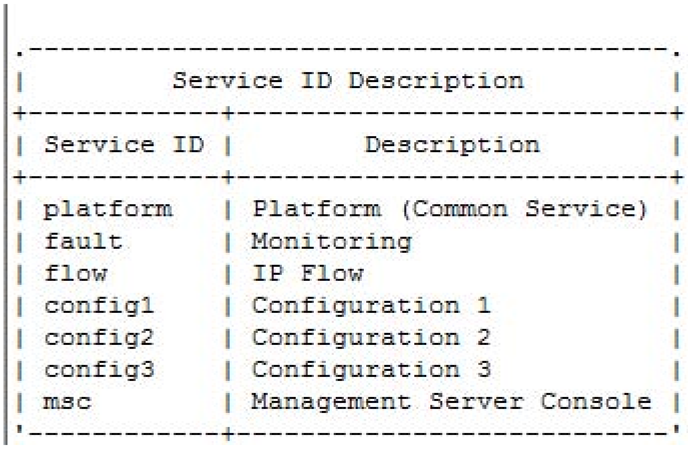
Cause

Unexpected errors, failure of any application, or sometime the application might fail, but you do not want to stop everything.

Solution

1. Run the **`afo-service-help`** command on the Command Line Interface (CLI) .

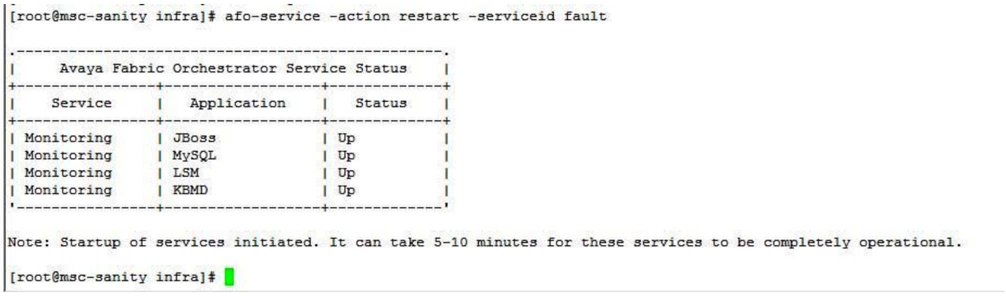
   The help menu displays the list of service ID along with their description.



```
.-----------------------------------------.
|         Service ID Description          |
+------------+----------------------------+
| Service ID |        Description         |
+------------+----------------------------+
| platform   | Platform (Common Service)  |
| fault      | Monitoring                 |
| flow       | IP Flow                    |
| config1    | Configuration 1            |
| config2    | Configuration 2            |
| config3    | Configuration 3            |
| msc        | Management Server Console  |
'------------+----------------------------'
```

Figure 5: Sample Output: Help command

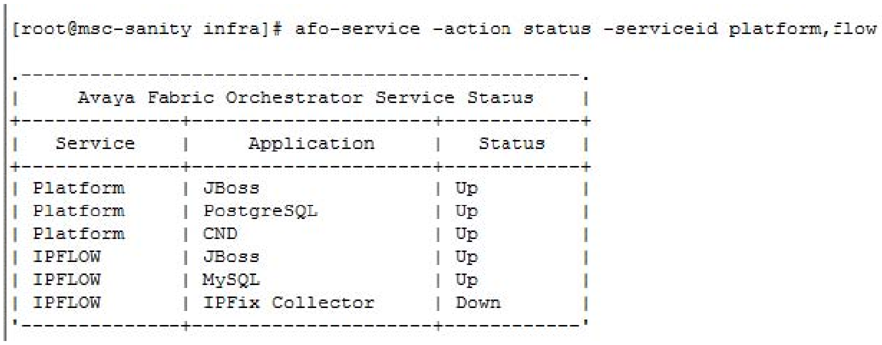
2. Run the **`afo-service -action <restart> -serviceid <Service>`** command to restart the application service on a particular virtual machine.



```
[root@msc-sanity infra]# afo-service -action restart -serviceid fault

.---------------------------------------------.
|     Avaya Fabric Orchestrator Service Status  |
+---------------+----------------+------------+
|    Service    |   Application  |   Status   |
+---------------+----------------+------------+
| Monitoring    | JBoss          | Up         |
| Monitoring    | MySQL          | Up         |
| Monitoring    | LSM            | Up         |
| Monitoring    | KBMD           | Up         |
'---------------+----------------+------------'

Note: Startup of services initiated. It can take 5-10 minutes for these services to be completely operational.

[root@msc-sanity infra]#
```

Figure 6: Sample Output: Command to restart the application service on a particular virtual machine

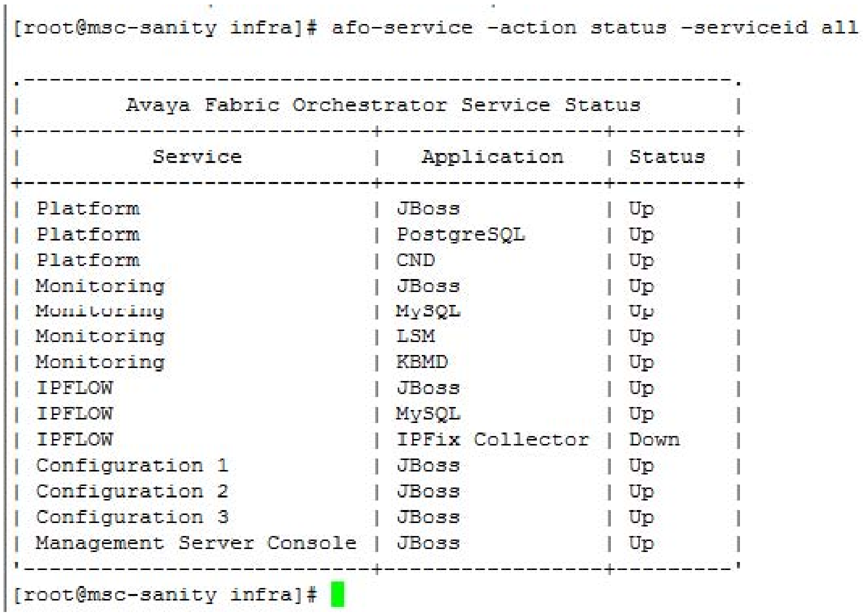
3. **(Optional)** Run the **`afo-service -action <status> -serviceid <Service 1, Service 2>`** command to view the application service status on multiple virtual machines.



```
[root@msc-sanity infra]# afo-service -action status -serviceid platform,flow

.--------------------------------------------------.
|     Avaya Fabric Orchestrator Service Status     |
+--------------+---------------------+-------------+
|   Service    |     Application     |   Status    |
+--------------+---------------------+-------------+
| Platform     | JBoss               | Up          |
| Platform     | PostgreSQL          | Up          |
| Platform     | CND                 | Up          |
| IPFLOW       | JBoss               | Up          |
| IPFLOW       | MySQL               | Up          |
| IPFLOW       | IPFix Collector     | Down        |
'--------------+---------------------+-------------'
```

Figure 7: Sample Output: Command to view status on multiple virtual machines

4. Run the **`afo-service -action <status> -serviceid all`** command to view the application service status on all the virtual machines.



```
[root@msc-sanity infra]# afo-service -action status -serviceid all

.-------------------------------------------------------.
|        Avaya Fabric Orchestrator Service Status       |
+---------------------------+-----------------+---------+
|          Service          |   Application   | Status  |
+---------------------------+-----------------+---------+
| Platform                  | JBoss           | Up      |
| Platform                  | PostgreSQL      | Up      |
| Platform                  | CND             | Up      |
| Monitoring                | JBoss           | Up      |
| Monitoring                | MySQL           | Up      |
| Monitoring                | LSM             | Up      |
| Monitoring                | KBMD            | Up      |
| IPFLOW                    | JBoss           | Up      |
| IPFLOW                    | MySQL           | Up      |
| IPFLOW                    | IPFix Collector | Down    |
| Configuration 1           | JBoss           | Up      |
| Configuration 2           | JBoss           | Up      |
| Configuration 3           | JBoss           | Up      |
| Management Server Console | JBoss           | Up      |
'---------------------------+-----------------+---------'
[root@msc-sanity infra]#
```

Figure 8: Sample Output: Command to view status on all the virtual machines

Hardware Resource Usage

You can use the Hardware Resource Usage utility to provide the current CPU and memory usage of each virtual machine on the AFO. This utility is present on the Management Server Console (MSC).

Condition

The unnoticed or inefficient method of tracking the hardware resource usage.

Cause

Excessive CPU and memory usage of the virtual machines.

Solution

1. Login to MSC as a user with administrative privileges.

   Note:

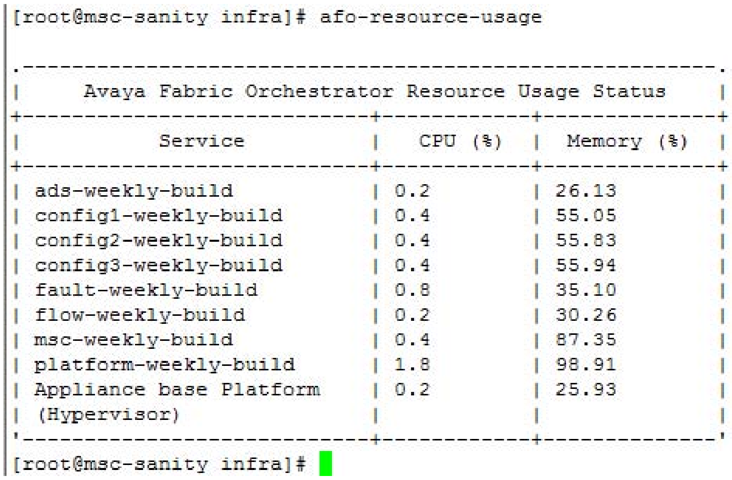
   You can enter default user name and password as `admin/Afo_123` to login.

2. Run the **`su - root`** command on the Command Line Interface (CLI) and switch to root user.

   Enter `Avaya_123` as default root password.

3. Run the **`afo-resource-usage`** command.

   The system displays the resource usage status of all the services deployed on AFO.



```
[root@msc-sanity infra]# afo-resource-usage

.--------------------------------------------------------.
|     Avaya Fabric Orchestrator Resource Usage Status     |
+----------------------------+------------+--------------+
|          Service           |  CPU (%)   |  Memory (%)  |
+----------------------------+------------+--------------+
| ads-weekly-build           | 0.2        | 26.13        |
| config1-weekly-build       | 0.4        | 55.05        |
| config2-weekly-build       | 0.4        | 55.83        |
| config3-weekly-build       | 0.4        | 55.94        |
| fault-weekly-build         | 0.8        | 35.10        |
| flow-weekly-build          | 0.2        | 30.26        |
| msc-weekly-build           | 0.4        | 87.35        |
| platform-weekly-build      | 1.8        | 98.91        |
| Appliance base Platform    | 0.2        | 25.93        |
|  (Hypervisor)              |            |              |
'----------------------------+------------+--------------'
[root@msc-sanity infra]#
```

Figure 9: Sample Output: Hardware Resource Usage Command

AFO Health Check

The AFO Health Check utility allows you to check the status of the applications running on each virtual machine. AFO Health Check utility discover the unhealthy application, to prevent jobs from being scheduled or run on them. Thus, increasing the reliability and throughput of the AFO cluster by reducing preventable job failures due to misconfiguration, hardware failure, etc.

Condition

Service request (Job) failure due to misconfiguration or application failure.

Cause

On AFO, multiple applications run continuously and exists on each virtual machine and handles periodic service requests that the system expects to receive.

Solution

1. Login to MSC as a user with administrative privileges.

   Note:

   You can enter default user name and password as `admin/Afo_123` to login.

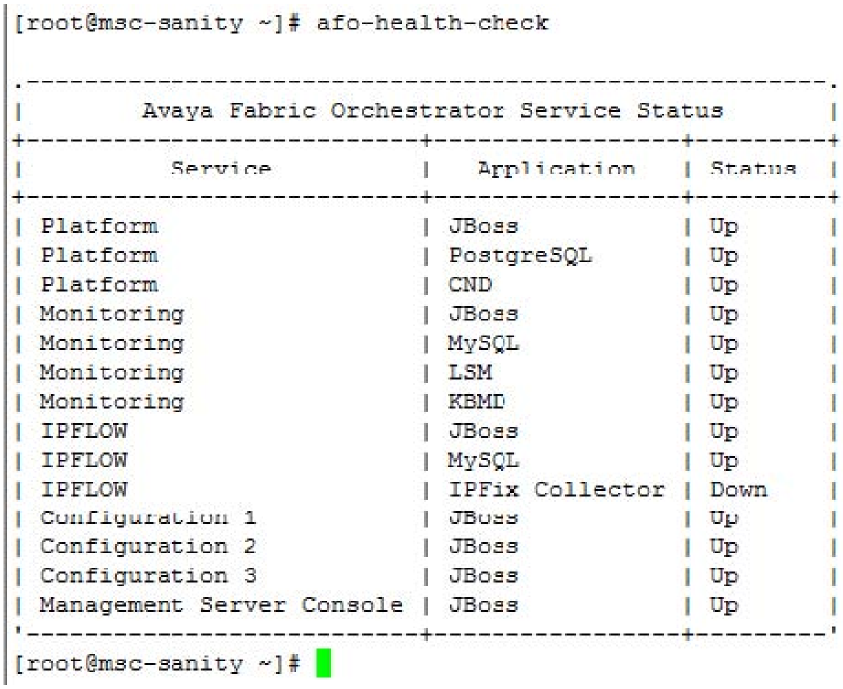
2. Run the **`su - root`** command on the Command Line Interface (CLI) and switch to root user.

   Enter `Avaya_123` as default root password.

3. Run the **`afo-health-check`** command.

   The system displays the health check status of all the applications deployed on AFO, in the `Status` column:

Status	Description
UP	Displays the status as `UP`, if the application is running
Down	Displays the status as `Down`, if the application is down



```
[root@msc-sanity ~]# afo-health-check

.----------------------------------------------------------.
|         Avaya Fabric Orchestrator Service Status         |
+-----------------------------+------------------+---------+
|           Service           |   Application    | Status  |
+-----------------------------+------------------+---------+
| Platform                    | JBoss            | Up      |
| Platform                    | PostgreSQL       | Up      |
| Platform                    | CND              | Up      |
| Monitoring                  | JBoss            | Up      |
| Monitoring                  | MySQL            | Up      |
| Monitoring                  | LSM              | Up      |
| Monitoring                  | KBMD             | Up      |
| IPFLOW                      | JBoss            | Up      |
| IPFLOW                      | MySQL            | Up      |
| IPFLOW                      | IPFix Collector  | Down    |
| Configuration 1             | JBoss            | Up      |
| Configuration 2             | JBoss            | Up      |
| Configuration 3             | JBoss            | Up      |
| Management Server Console   | JBoss            | Up      |
'-----------------------------+------------------+---------'
[root@msc-sanity ~]#
```

Figure 10: Sample Output: AFO Health Check Command

Factory Reset

The Avaya Fabric Orchestrator (AFO) Factory Reset utility allows you to re-deploy AFO on the server. Before you perform a Factory Reset, ensure that you have taken a backup of the existing data.

⚠ **Warning:**

The AFO Factory Reset utility will bring back the server into the same state of the factory build, and all the existing data will be erased.

Note:

Avaya recommends to backup the data before performing AFO Factory Reset.

Condition

If the AFO device is in an unusable state, and you are not able to troubleshoot.

⚠ **Caution:**

Contact Avaya support center before performing AFO Factory Reset.

Solution

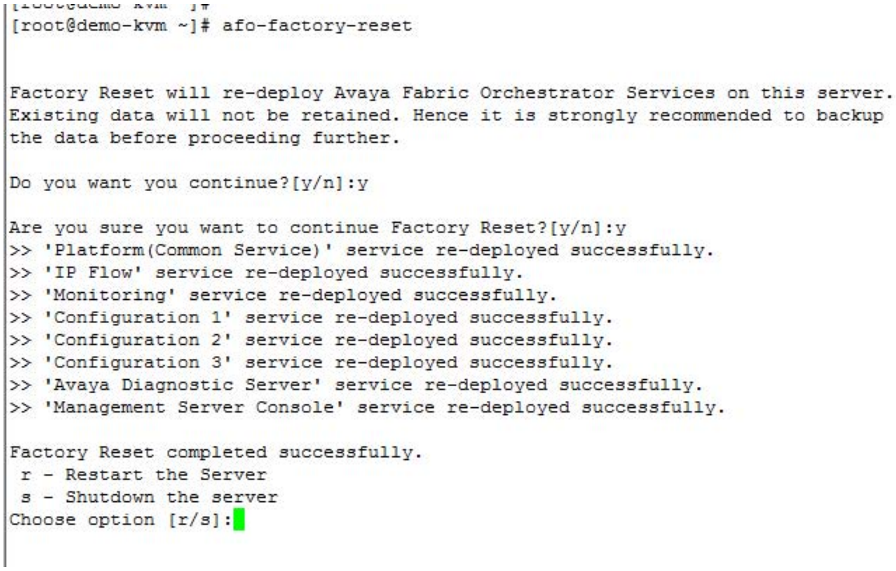
1. Login to Appliance base Platform (Hypervisor) as a root user.
2. Run the **`afo-factory-reset`** command on the Command Line Interface.

   The system prompts you to confirm before it starts the factory reset procedure.

Choice Option	Choice Description
`y`	Enter `y` to continue the reset
`n`	Enter `n` to cancel the reset

3. The system prompts you to either restart the server to begin the configuration or shutdown the server to configure later.

Choice Option	Choice Description
`r`	Enter `r` to restart the server to begin the configuration
`s`	Enter `s` to shutdown the server to configure later



```
[root@demo-kvm ~]# afo-factory-reset


Factory Reset will re-deploy Avaya Fabric Orchestrator Services on this server.
Existing data will not be retained. Hence it is strongly recommended to backup
the data before proceeding further.

Do you want you continue?[y/n]:y

Are you sure you want to continue Factory Reset?[y/n]:y
>> 'Platform(Common Service)' service re-deployed successfully.
>> 'IP Flow' service re-deployed successfully.
>> 'Monitoring' service re-deployed successfully.
>> 'Configuration 1' service re-deployed successfully.
>> 'Configuration 2' service re-deployed successfully.
>> 'Configuration 3' service re-deployed successfully.
>> 'Avaya Diagnostic Server' service re-deployed successfully.
>> 'Management Server Console' service re-deployed successfully.

Factory Reset completed successfully.
 r - Restart the Server
 s - Shutdown the server
Choose option [r/s]:
```

Figure 11: Sample Output: AFO Factory Reset Command

FAQs

Q:

What are the benefits of a Avaya Fabric Orchestrator (AFO) hardware appliance?

A:

A hardware appliance reduces the number of SKUs that you need to order for an integrated management solution and eliminates the need to maintain and configure your servers.

Avaya Fabric Orchestrator (AFO) is a virtualized solution inside a pre-configured hardware that makes it easier to patch and upgrade.

Q:

How do customers install the Avaya Fabric Orchestrator (AFO) appliance on their network?

A:

First-boot deployment scripts will ask you a series of questions related to the networking as well as the application, and will auto-configure the appliance and virtual machines. For more information, see *Deploying Avaya Fabric Orchestrator*, NN48100–101.

Q:

How to upgrade for customers who have already purchased maintenance contracts for COM, VPS, or VPFM?

A:

If you are an existing customer with existing maintenance contracts for COM, VPS, or VPFM, you will be able to purchase CF Controller appliance (without add-ons) for a discounted price. For more information on data migration from existing application to AFO, see *Deploying Avaya Fabric Orchestrator*, NN48100–101.

Q:

How will customers be able to upgrade AFO in the future?

A:

The AFO appliance includes a Management Server Console application that will help monitor the state of the various virtual machines on the appliance and help to upgrade the virtual machines.

Q:

Can customers deploy their virtual machines on the AFO appliance?

A:

No. You cannot deploy any other virtual machines other than AFO and add-ons on the appliance, as AFO is a closed system.

Q:

Will customers be able to manage the CF Controller appliance using vCenter?

A:

The appliance will not include vCenter. Although you can use your existing vCenter to manage the appliance. As noted above, the appliance is a closed system, and the management virtual machines are not allowed to migrate out of the appliance, and neither any other virtual machines be able to migrate into this appliance.

Chapter 15: Maintenance

AFO system Backup

About AFO Backup

Maintaining backup files can minimize downtime if AFO system information becomes corrupt.

Backup Options

- You can perform AFO system backup manually or can perform a scheduled backup at specific time interval.
  - **Manually** : AFO does not perform automatic backups. You can manually backup the AFO system using the command line interface (CLI). For more information on how to perform a manual backup of the system, see Performing a Manual AFO Backup on page 139.
  - **Scheduled**: You can perform scheduled AFO backups at the specific time specified in the day and hour graph. Scheduled backups occur at regular intervals, or at selected days of the week and time. By default, the backup is scheduled for every Sunday at 22:00 hours.

Recommendations

Use the information in this section to understand the considerations and recommendations before performing a manual AFO backup.

- You can perform a health check using the Command Line Interface (CLI) to check the status of all the virtual machines (VMs) and applications on AFO.

Guidelines and Limitations

The following are guidelines and limitations to use when backing up and recovering a AFO system:

- You can perform backup and restore of application related data, common services, and platform data only through Command Line Interface (CLI).

  Note:

  Partial backup and restore of the AFO system is not allowed. The AFO system performs the entire backup and restore of the applications at once.

- You cannot perform backup and restore if any of the virtual machine is corrupted.

Flowchart: Performing a Manual AFO Backup

You can use the following process for performing a manual backup of the AFO system.

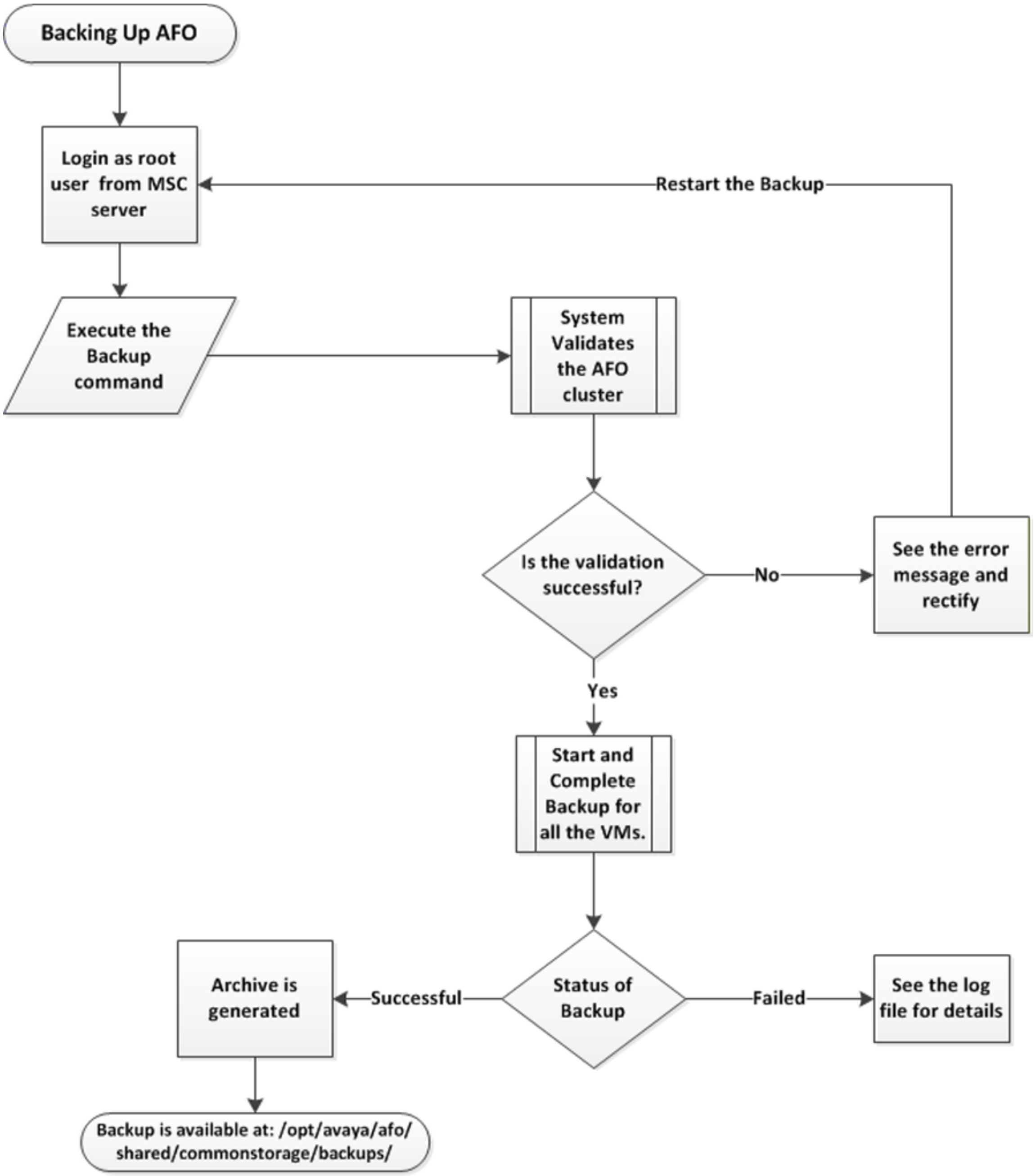

Backing Up AFO
Login as root user from MSC server
Restart the Backup
Execute the Backup command
System Validates the AFO cluster
Is the validation successful?
No
See the error message and rectify
Yes
Start and Complete Backup for all the VMs.
Status of Backup
Successful
Failed
Archive is generated
See the log file for details
Backup is available at: /opt/avaya/afo/shared/commonstorage/backups/

Figure 12: Flowchart: Performing a Manual AFO Backup

Performing a Manual AFO Backup

About this task

You can perform a manual backup whenever you want, without scheduling the backup. Use the following procedure to perform a manual backup of the AFO system using the command line interface (CLI).

Before you begin

- Ensure that you are logged on to the MSC server.
- Enter `root username` and `password`.

Procedure

1. Login as a root user on the MSC server.
2. Run the backup command:

   `/opt/avaya/smgr/backuprestore/backupRestoreAFO.sh --backup`
3. The system validates the AFO cluster for backup procedure.
   - If validation is successful go to step 5.
   - Else, see the error message and rectify and go to step 1.
4. The system proceeds with a backup of AFO when the validation is successful.
5. The system displays the status of the backup and creates an archive at `/opt/avaya/afo/shared/commonstorage/backups/` if the status is `Successful`.

   Archive does not include backup of any add-ons deployed on the AFO cluster.

   Note:

   Refer to the log file located at `/opt/avaya/smgr/log/AFOBackupRestore.log` for more details if the system `Failed` to take backup.

Example

Backup command:

```
/opt/avaya/smgr/backuprestore/backupRestoreAFO.sh --backup
```

The system validates the cluster for the backup procedure and starts a backup of all the applications if the validation is `successful`:

```

Validation is successful.
Proceeding with backup of AFO.

Started backup of AFO.
This procedure will take some time.

...
Completed backup of Msc service on app7-clus1-msc.blr.avaya.com


Completed backup of Flow service on app7-clus1-flow.blr.avaya.com


Completed backup of Config service on app7-clus1-config3.blr.avaya.com


Completed backup of Config service on app7-clus1-config2.blr.avaya.com
...

Completed backup of Config service on app7-clus1-config1.blr.avaya.com
.........

Completed backup of Fault service on app7-clus1-fault.blr.avaya.com
```

```
...............

Completed backup of Platform service on app7-clus1-platform.blr.avaya.com

------------------------------------------------------------------
------------
Service
  Server                                  Status
------------------------------------------------------------------------------
Platform
 app7-clus1-platform.blr.avaya.com      Completed
Fault
app7-clus1-fault.blr.avaya.com         Completed(with warnings)
Flow
app7-clus1-flow.blr.avaya.com          Completed
Config
app7-clus1-config1.blr.avaya.com       Completed(with warnings)
Config
app7-clus1-config2.blr.avaya.com       Completed(with warnings)
Config
app7-clus1-config3.blr.avaya.com       Completed(with warnings)Msc
app7-clus1-msc.blr.avaya.com           Completed
------------------------------------------------------------------------------
```

The system creates an archive:

```
Status of backup : Successful
Creating archive...
Backup is available at: /opt/avaya/afo/shared/commonstorage/backups/
AFOBackup_2015-05-21_07.04.zip.
```

If the validation is `Successful`, but the system failed to take backup on the server:

```
Validating the AFO cluster for backup procedure.

Validation is successful. Proceeding with backup of AFO.

Started backup of AFO.
This procedure will take some time.
Failed to take backup on server : Msc service on app7-clus1-msc.blr.avaya.com

Completed backup of Flow service on app7-clus1-flow.blr.avaya.com


Completed backup of Config service on app7-clus1-config3.blr.avaya.com


Completed backup of Config service on app7-clus1-config2.blr.avaya.com
...

Completed backup of Config service on app7-clus1-config1.blr.avaya.com
......

Completed backup of Fault service on app7-clus1-fault.blr.avaya.com
..................

Completed backup of Platform service on app7-clus1-platform.blr.avaya.com

------------------------------------------------------------------------------
Service
  Server                                  Status
------------------------------------------------------------------------------
Platform
```

```
app7-clus1-platform.blr.avaya.com      Completed
Fault
app7-clus1-fault.blr.avaya.com         Completed(with warnings)
Flow
app7-clus1-flow.blr.avaya.com          Completed
Config
app7-clus1-config1.blr.avaya.com       Completed(with warnings)
Config
 app7-clus1-config2.blr.avaya.com       Completed(with warnings)
Config
app7-clus1-config3.blr.avaya.com       Completed(with warnings)
Msc
 app7-clus1-msc.blr.avaya.com           Error
------------------------------------------------------------------------------

Status of backup : Failed
```

Refer to the log file:

```
Please refer to the log file located at '/opt/avaya/smgr/log/AFOBackupRestore.log' for
more details.
```

AFO system Restore

Flowchart: Performing a AFO Restore

You can use the following process for restoring a AFO system.

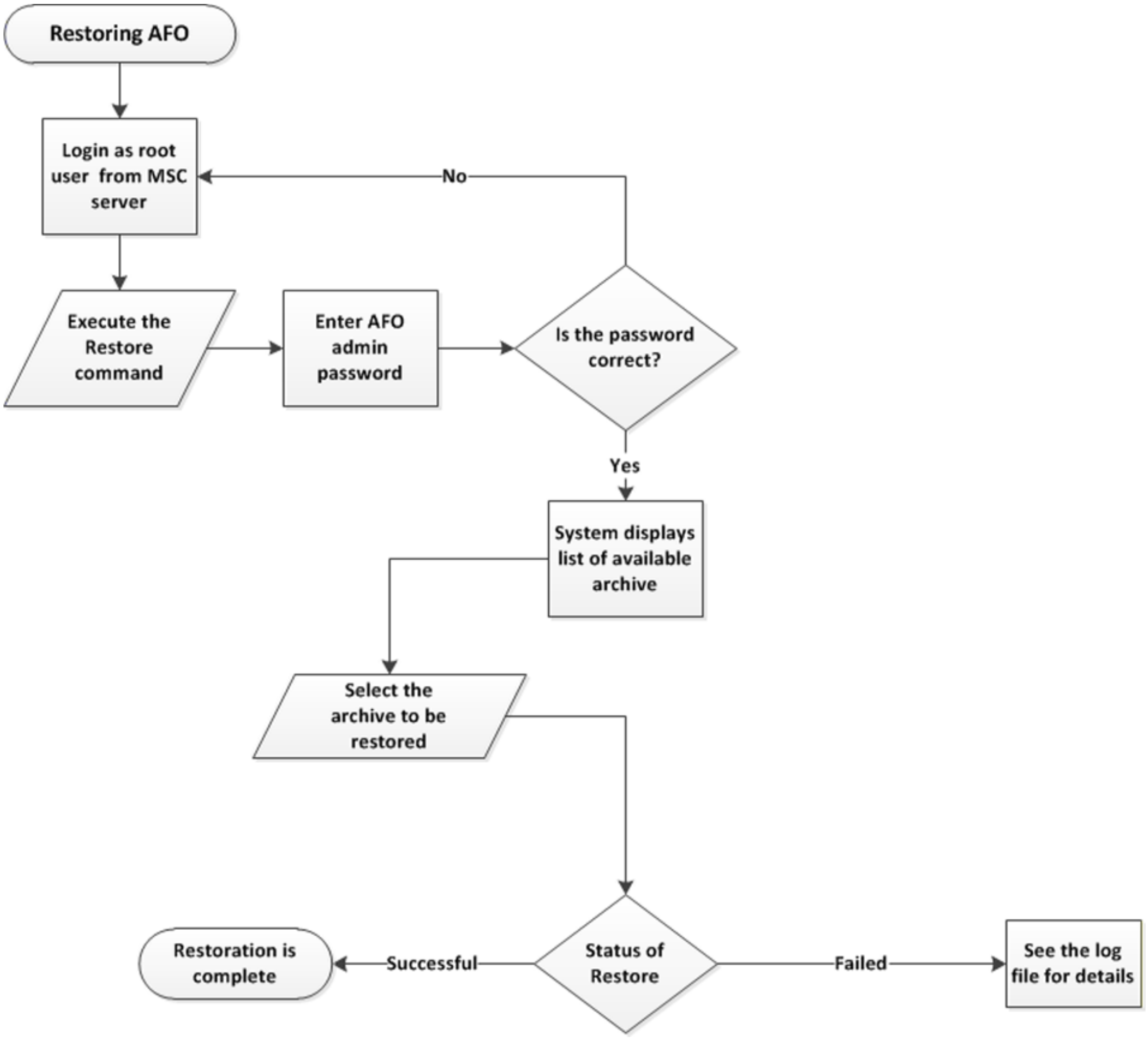

Restoring AFO
Login as root user from MSC server
No
Execute the Restore command
Enter AFO admin password
Is the password correct?
Yes
System displays list of available archive
Select the archive to be restored
Restoration is complete
Successful
Status of Restore
Failed
See the log file for details

Figure 13: Flowchart: Performing a AFO Restore

Restoring AFO

About this task

You can perform a system restoration of AFO whenever needed. Use the following procedure to restore AFO from a backup archive.

Before you begin

- Ensure that you are logged on to the MSC server as a root user.

Procedure

1. Run the restore command:

```
/opt/avaya/smgr/backuprestore/backupRestoreAFO.sh --restore
```

2. Enter AFO admin password.

   The system displays the list of the archives available to restore.
3. Enter an archive from the list to restore.
4. The system validates the archive details.

Choice Option	Choice Description
y	Enter `Y` to proceed
N	Enter `N` to cancel the restore

5. The system automatically validates the AFO cluster for restore procedure and proceeds with restore after the successful completion of the validation.
6. The system displays the status of restore as `Successful` or `Failed`.

   Note:

   Refer to the log file located at `/opt/avaya/smgr/log/AFOBackupRestore.log` for more details if the status is `Failed`.

Example

Restore command:

```
 /opt/avaya/smgr/backuprestore/backupRestoreAFO.sh --restore
```

The system displays a list of the archives for restore:

```
Enter AFO admin password: *********

The following archives are available to restore.
Please choose from the list.

1. AFOBackup_2015-05-18_15.01.zip

2. AFOBackup_2015-05-18_15.56.zip

3. 2015-04-24_03.06.zip

4. AFOBackup_2015-05-07_13.10.zip

5. AFOBackup_2015-05-18_15.04.zip
```

Select an archive:

```
Please choose an archive.
2
You have chosen : AFOBackup_2015-05-18_15.56.zip.
Do you want to proceed? (yes/no)
y
**************************************************************************
WARNING: You have chosen to restore the AFO cluster. This will replace the whole data
which cannot be reverted.
Do you want to proceed (y/n)?
y
**************************************************************************
Validating the AFO cluster for restore procedure.
Validation is successful.
 Proceeding with restore of AFO.
```

```
Restore of AFO has been started.
This procedure will take some time.
```

The system executes restore procedure for each of the applications for a selected archive:

```
Executing restore of Platform service on app7-clus1-platform.blr.avaya.com
Restoration is complete for Platform service on app7-clus1-platform.blr.avaya.com

Executing restore of Fault service on app7-clus1-fault.blr.avaya.com
................................................
Restoration is complete for Fault service on app7-clus1-fault.blr.avaya.com


Executing restore of Config service on app7-clus1-config1.blr.avaya.com

Executing restore of Flow service on app7-clus1-flow.blr.avaya.com
...

Restoration is completed for Msc service on app7-clus1-msc.blr.avaya.com


Restoration is complete for Flow service on app7-clus1-flow.blr.avaya.com

..........................................................................................
..........................................................................................
..........................................................................................
................................................

Restoration is complete for Config service on app7-clus1-config1.blr.avaya.com


Executing restore of Config service on app7-clus1-config2.blr.avaya.com
..........................................................................................
..........................................................................................
..........................................................................................
.............................................
Restoration is complete for Config service on app7-clus1-config2.blr.avaya.com

Executing restore of Config service on app7-clus1-config3.blr.avaya.com
..........................................................................................
..........................................................................................
..........................................................................................
.............................................
Restoration is complete for Config service on app7-clus1-config3.blr.avaya.com


------------------------------------------------------------------------------
Service       Server                                  Status
------------------------------------------------------------------------------
Platform
app7-clus1-platform.blr.avaya.com      Completed
Fault
app7-clus1-fault.blr.avaya.com         Completed(with warnings)
Flow
app7-clus1-flow.blr.avaya.com          Completed
Config
app7-clus1-config1.blr.avaya.com       Completed(with warnings)
Config
app7-clus1-config2.blr.avaya.com       Completed(with warnings)
Config
app7-clus1-config3.blr.avaya.com       Completed(with warnings)
Msc
```

```
 app7-clus1-msc.blr.avaya.com           Completed
----

Status of restore : Successful
```

Viewing an archive

About this task

Use this task to view the details of an archive.

Before you begin

Ensure that you have perform the backup of the AFO system.

Procedure

Run the following command to view the details of an archive.

```
/opt/avaya/smgr/backuprestore/backupRestoreAFO.sh --view
```

Appendix A: Solution Software Director Overview

You can perform software upgrade and patching using Solution Software Director (SSD) using the AFO web interface.

On the AFO menu bar, click **Administration** > **Solution Software Director** to perform a software upgrade. The system displays the SSD home page that contain the following sections:

Table 13: SSD Home page web interface description

SSD Home page element		Description
Toolbar	Home	Use SSD home page to perform software upgrade and patching. Click **Home** from the top toolbar to open the SSD home page.
	MSC Preferences	Helps to add and define MSC settings and other properties of the AFO across multiple sessions. **Tip:** You can also launch **MSC Preferences** from the AFO quick access toolbar. Click Preferences icon from the quick access toolbar to open the **MSC Preferences** page.
	Software Library	Serves as a repository of software bundles. • Upload software bundles in an offline mode for upgrade. • In an online mode, bundles get automatically downloaded here.
	Upgrade History	Shows the history of upgrades performed on this AFO appliance in reverse chronological order. Information of the last upgrade is shown on the top.

Table continues…

SSD Home page element		Description
System information	AFO Release	Displays current release number of the AFO system.
	License	Displays the current License type of the AFO system.
System Status	Application Status	Displays if the application status is `Online` or `Offline`, based on the availability of PLDS access, from the server.

You can upgrade the software using any one of the following method:

- Perform Upgrade in Easy Mode: For more information, see Easy mode upgrade on page 118.
- Perform Upgrade in Advanced Mode: For more information, see Advanced mode upgrade on page 120.

Activity Logs

Activity Logs is the common section across all the pages of the SSD. **Activity Logs** provide runtime updates of the upgrade activities to all logged in users of the AFO SSD at that point in time. Log messages of the current upgrade activities performed by an administrator is visible to all the users who are logged into SSD at that time.

Note:

Activity Logs pane displays all the error messages in red color text.

You can use the **Activity Logs** pane to perform the following tasks:

- Clear activity logs
- Save activity logs

Software Library

Software Library serves as a repository of software bundles. You can work with software bundle in online mode as well as offline mode.

- In an offline mode, you can upload software bundles for upgrade.
- In an online mode, bundles get automatically downloaded here.

You can launch Software Library in the following two ways:

- Launch **Software Library** from the SSD home page top toolbar.
- Or launch **SSD** > **Work Flow** > **Utilities** > **S/W Library**.

Inventory

When you click **Perform upgrade in Advanced mode** on the landing page, the **Inventory** page displays. **Inventory** page displays the current list of each service; **Name, IP address, Type, and Version** running on the system.

On the **Inventory** page, the system displays either the **Upload Matrix** or **Analysis** button based on the PLDS connectivity from the server.

When PLDS is not accessible from server (offline)

1. Click **Upload Matrix** to get updated recommendation for upgrades.

   The system displays the **Wizard EULA** pop-up window.
2. Select **I Agree the terms of License Agreement** and click **OK** to agree the license agreement to upload files pertaining to Avaya AFO upgrades.

When PLDS is accessible from server (online)

Click **Analysis** to perform the analysis to retrieve the latest available releases for the upgrade.

Analysis

The **Analysis** page displays the latest recommended release based on the analysis in the **Release** drop-down column.

Select the Release. The color-code near the **Name** column is displayed.

The following table provides the list of color code and their significance:

Table 14: Color-code significance

Color Code	Description
Green	No new upgrade or update is available. The system is already up-to-date.
Red	Compatible upgrade or update is available on PLDS but not available in the **Software Library**.
Yellow	Compatible upgrade or update is available in the **Software Library** (both online and offline mode).
Purple	Compatible upgrade or update is available on PLDS. However, you are not entitled to an upgrade.
Grey	Analysis has not been run. Perform **Analysis**.

On the **Analysis** page, the system displays the **Upload Bundle** or **Download Bundle** button depending on the accessibility from the server.

- Upload Bundle- displays when PLDS is not accessible from server (offline).
- Download Bundle- displays when PLDS is accessible from server (online).

Precheck

The **Precheck** page displays the results on a per service basis as `Pass` or `Fail` along with the description. Perform the prerequisite check of the downloaded or uploaded bundles.

Note:

If any service pre-checks fail, the upgrade is blocked from the execution. See the **Activity Logs** section to rectify the problem before you perform an upgrade.

Tip:

Activity Logs provide runtime updates of the upgrade activities to all logged in users of the AFO SSD at that point in time.

Upgrade

The **Upgrade** page displays the **Download ID, File Name, Short Description, and Progress** of the upgrade. The **Progress** column displays a green color bar when the upgrade status is complete.

Note:

The **Upgrade** is enabled only after the successful completion of the pre-checks. If any service pre-checks fail on the **Precheck** page, the upgrade is blocked from the execution.

Downloading a bundle

About this task

You can perform this task to download a bundle. The **Download** page displays only when PLDS is online and accessible from the server.

Procedure

1. Click **Download Bundle**.

   The system automatically downloads the bundles required for the upgrade from the PLDS.

   Note:

   The system also automatically downloads the latest compatibility matrix from the Avaya FTP site. The **Software Library** page serves as a repository to store these bundles and compatibility matrix XML files.

2. Click Precheck on page 150 to perform the prerequisite check of the downloaded bundles.

Uploading a bundle

About this task

Perform this task to upload the bundles required for the upgrade along with their availability. The **Upload Bundle** page displays when PLDS is not accessible from the server and is offline.

Procedure

1. If the requisite bundles are already available in the **Software Library**:

   Browse column is disabled and **Progress** column displays a status as **File is available**.
2. If the requisite bundles are not available in the **Software Library**:

   Click **Browse** to upload the bundle and Click **Start Upload**.
3. Click Precheck on page 150 to perform the prerequisite check of the uploaded bundles.

Uploading a compatibility matrix

About this task

Perform this task to upload the latest compatibility matrix file so that the system identifies the latest and their requisite bundle information.

✱ **Note:**

The system displays **Upload Compatibility Matrix** page only when PLDS is offline.

Procedure

1. On the **Upload Compatibility Matrix** page, click **Browse** to upload compatibility matrix to get updated recommendation.

   ✱ **Note:**

   If the latest compatibility matrix is unavailable on the system, download the latest compatibility matrix in the software library from the Avaya Support Site when PLDS server is online.
2. Click **Upload**.

   The system displays a `success` or a `failure` message for the file uploaded.
3. Click Analysis on page 149 if the file is successfully uploaded.

   The system performs the analysis to retrieve the latest available releases for the upgrade.