Administration using Avaya Fabric Orchestrator

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

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

License types

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see

the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction

Purpose

This document contains concepts, operations, and tasks related to the management features of the Avaya Fabric Orchestrator (AFO). This guide also describes additional administrative tasks such as backups, software updates, and preferences.

Chapter 2: New in this document

The following sections detail what is new in *Administration using Avaya Fabric Orchestrator*, NN48100–600. See *Avaya Fabric Orchestrator Release Notes* for a list of supported features.

Release 1.1

Customizable dashboard

The Home dashboard provides a real-time statistical view of the various applications integrated on the system in the form of widgets. The widgets are dynamic components that display live feeds of the applications. You can add, edit, move, and delete the dashboard widgets and customize them to fit your needs.

For more information, see Customizable dashboard on page 21.

Device licensing

Device licensing lets you perform legacy license discovery from the devices in the network.

For more information, see Device licensing on page 142.

North Bound Interface (NBI) Access Control

AFO Release 1.1 supports the NBI Access control. NBI Access Control is a module, that enforces control and allows which user can access which API methods.

For more information, see NBI Access Control Overview on page 145.

VxLAN Tunnel Management

VxLAN is an overlay networking protocol that disassociates workloads from physical networks, allowing for possible transition to the cloud-based providers. You can use VxLAN Manager to configure the VxLAN tunnels on the Avaya VxLAN capable devices and to manage the VxLAN tunnels in the network.

To access, login to the AFO GUI and navigate to **Configuration** > **VxLAN**.

This feature is available on VSP8xxx and VSP72xx running on VOSS v6.0 release.

Device License Manager

AFO Release 1.1 allows you to manage all Avaya network devices from a user interface which resides in AFO. Use Device License Manager to view the list of capable devices and to discover device license information.

To access Device License Manager, login to the AFO GUI and navigate to **Administration** > **Device Licensing**.

RESTful Northbound API framework with OAuth 2.0 authorization support

AFO 1.1 provides support for Northbound APIs to retrieve basic information on the discovered devices. Avaya and third-party developed clients can access the APIs using OAuth-based 2.0 authorization. Access to the APIs is restricted only to registered clients and users of the Northbound Interface APIs. APIs filters and sorts the responses and displays in XML/JSON format.

The following table shows the Northbound web service APIs supported in this release:

API	Description
Discovery API	1. Provides the list of all the domains 2. Provides statistics of the domain like number of ip phones, switches, routers etc.
Devices API	Provides list of devices present in a domain
Inventory API	Provides all the information about the device like port, power supply, fans, sensors, chassis etc.

High Availability

AFO provides a High Availability (HA) framework to support redundancy at the hardware, hypervisor, and application levels. AFO HA requires two physical appliances inter-connected through appliance port NIC3, and a HA license. AFO HA provides active-standby redundancy, all data on the Leader server is replicated to the Standby server to support failover.

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 the management applications.

Table 1: Network management applications

Application	Description
Configuration	Provides an intuitive interface to configure and manage the Avaya Enterprise family of devices from a discovered network.
Bulk Provisioning	Provides the tools to perform a variety of management tasks across multiple device types using a web-based interface.
Monitoring	Monitors the managed objects and reduces troubleshooting issues because of a more complete view of the network.
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.
Virtualization	Connects the vCenter server to the configuration application to help the data center administrator configure the network changes that apply to the data center. Monitors the virtual infrastructure and provisions the network.

Chapter 4: Administration tools

Administration tools overview

You can manage the appliance and various features through the following administration tools:

- Web interface
- Command line interface (CLI)

Web interface

You can view the web interface using Microsoft Internet Explorer, version 11, Mozilla Firefox, versions 47 and later, or Safari (macOS v10.8 Mountain Lion and later). The web interface provides you with an improved user experience with data-driven menus for easy integration with current applications and future add-ons.

The Home page displays as the landing page and provides a dashboard with a customizable view of the system. You can use the Home page to determine the operating status of the various management functions in your configuration. You can return to the Home page at any time during your session. To return to this page, click the product name on the menu bar.

The following figure shows the overall sections of the web interface.

Administration tools
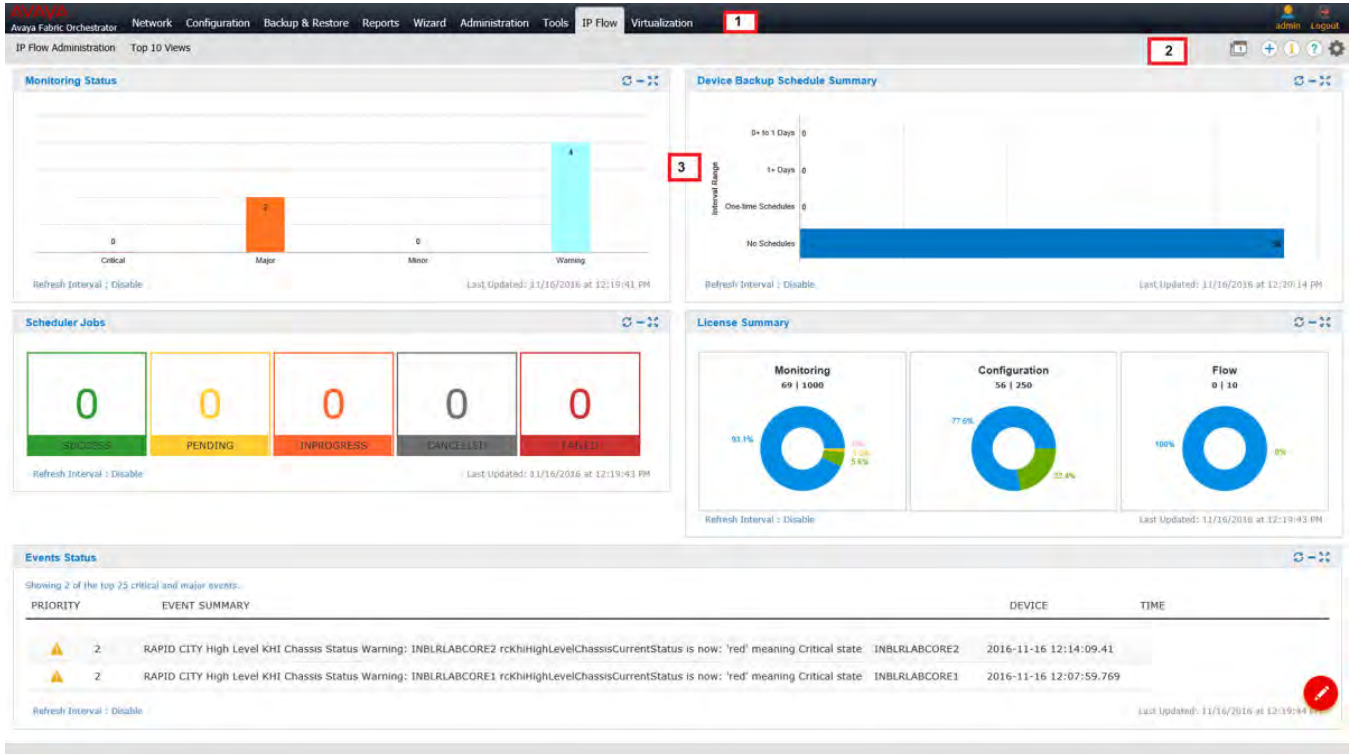
Table 2: Home page

No.	Name	Description
1	Menu bar	Provides the navigation options for the system. The area at the top of the 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 • Virtualization

Table continues…

No.	Name	Description
2	Quick access toolbar	Provides quick access to commonly used 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	Home dashboard	Provides a customizable view of the system.

Web interface icons

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

Table 3: Common icons

Icon	Name	Description
	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:** Tab Scope displays the latest 12 tabs that includes HOME tab, which cannot be removed. 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

Table continues…

Icon	Name	Description
	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	Use Logout to exit from the application.

Logging on to the web interface

About this task

Use this procedure to log on to the web interface for the first time.

Before you begin

Ensure that you have:

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

✳ Note:

Make sure that the FQDN is registered on your DNS server or add an entry in the hosts file of the machine that you use to access the system.

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 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 web interface with the system `<version_number>`. The web interface displays the menu bar. The menu bar provides access to shared services to perform various operations that the system supports. The tasks that you can perform depend on your user role.

   - If the user name and password does not match, the system 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 password for the web interface.

🛈 **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 appliance.
- A computer with a supported Internet Explorer, Firefox, or Safari web browser, and access to the network where the 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 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 the system certificates.

Command Line Interface

You can use the command line interface (CLI) to administer and use some of the key features. The CLI provides a number of commands to perform the administrative and troubleshooting tasks.

Through the CLI, you can:

- Perform a factory reset.
- View the hardware resource usage.
- Perform a health check.
- Start, stop, or restart the application service.
- Update and edit the network configuration.
- Configure the NTP.
- Update the iLO settings.
- View the HA health status.
- View the Host ID

✳ **Note:**

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

CLI commands

The following table lists the CLI commands available through CLI:

You can run the following commands with root user credentials from the KVM hypervisor.

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

Service	Allows you to easily stop, start, or restart the application service.	• To view the help menu
		
		`cluster-service -help`
		
		• To stop the services in all VMs:
		
		`cluster-service -action stop -serviceid all`
		
		• To start services in all VMs:
		
		`cluster-service -action start -serviceid all`
		
		• To restart services in all VMs:
		
		`cluster-service -action restart -serviceid all`

Table continues…

Command	Description	Syntax

		• To check the status of all VMs:
		
		`cluster-service -action status -serviceid all`
		
		• To stop applications in a particular VM:
		
		`cluster-service -action stop -serviceid <platform|fault|flow| config|config1|config2| msc>`
		
		• To start applications in a particular VM:
		
		`cluster-service -action start -serviceid <platform|fault|flow| config|config1|config2| msc>`
		
		• To restart applications in a particular VM:
		
		`cluster-service -action restart -serviceid <platform|fault|flow| config|config1|config2| msc>`
		
		• To check the status of applications in a particular VM:
		
		`cluster-service -action status -serviceid <platform|fault|flow| config|config1|config2| msc>`
		
		• To configure the NTP
		
		`cluster-configure-ntp`
		
		• To update the iLO settings
		
		`cluster-update-iloinfo`

Network change	Allows you to update and change the network details post deployment.	`cluster-network-config`

Table continues…

Command	Description	Syntax
	⊛ **Note:** The process takes approximately 45 minutes to complete. ❗ **Important:** If you change the IP address or FQDN, during the next login you are prompted to change the password.	
Network information	Displays the hostname and IP address of all the virtual machines that are configured.	`cluster-info`
HostID	Provides the HostID for generating a license.	`cluster-hostid`
HA health status	Provides the HA health status at any given point of time.	`cluster-ha-status`

Chapter 5: Customizable dashboard

The Home page displays when you log in to the system and provides a dashboard with a customizable view of the system.

Click the product name on the menu bar to return to the Home dashboard at any time during your session.

Home dashboard overview

The Home dashboard provides a real-time statistical view of the various management functions on the system in the form of widgets. The widgets are dynamic components that display live feeds of the management functions. You can add, edit, move, and delete the dashboard widgets and customize them to fit your needs.

To customize the dashboard or add or change a widget, click the **Customize Dashboard** icon.

To access the dashboard, click the product name on the system menu bar.

The widgets that you can include on the dashboard depend on your product and licensing. The available widgets may include:

Widget	Description
Monitoring Status	Displays a summary of the monitoring status on the network. The Monitoring Status displays the number and severity of events. You can disable the poll interval or schedule a refresh at regular intervals.
License Summary	Displays the inventory details for the current license. The License Summary shows the number of used nodes or devices in relation to the total supported node/device count. You can disable the poll interval or schedule a refresh at regular intervals.
Scheduler Jobs	Tracks the state of bulk configuration tasks. Categorizes the tasks into Successful, Pending, In Progress, Cancelled, and Failed. Provides a view of the total number of scheduled jobs and the consolidated status. You can disable the poll interval or schedule a refresh at regular intervals.
IP Flow Pattern	Provides the flow details for the current license. You can disable the poll interval or schedule a refresh at regular intervals.
Event Status	Provides the top 25 messages from the monitoring function to get an overall view of the health of the system. Click the headings to arrange the list by

Table continues…

Widget	Description
	priority, message, device type, or time a message was received. You can disable the poll interval or schedule a refresh at regular intervals.
Device Backup Schedule Summary	Displays the number of devices that have a backup schedule interval in a given range. Also displays the number of devices that have no backup schedules and the devices with a backup schedule interval greater than the last specified interval range. You can disable the poll interval or schedule a refresh at regular intervals. You can configure the interval unit, size of range, and number of ranges to display in the summary. You can also choose to consider only active schedules.
Device Inventory	Displays the devices in the current setup. You can group the devices (by family, by family and model, or by family and software version), and expand or collapse groups to choose how many devices to display on the page. You can also filter and search for devices according to name, IP address, model, or software version.

The widget toolbar provides the quick access functionality for each widget. Some options are only available in edit mode after you select **Customize Dashboard**.

Icon	Name	Description
↻	**Refresh Widget**	Refreshes the content of the widget.
✛	**Change Widget Location**	Available in edit mode. Click and hold the icon to drag and drop the widget to a new location on the dashboard.
–	**Collapse Widget**	Collapses the widget on the dashboard so only the name and toolbar are visible. Click **+** to expand the widget.
⚙	**Configure Widget**	Available in edit mode. Opens the configuration settings for the widget.
⤢	**Fullscreen Widget**	Opens the widget on top of the dashboard and grays out the rest of the dashboard.
✖	**Remove Widget**	Available in edit mode. Removes the widget from the dashboard.

Customize Dashboard icons

The following table shows the icons available for Customize Dashboard.

Icon	Name	Description
✏	**Customize Dashboard**	Takes you to edit mode where you can customize the dashboard to suit your needs. Select **Apply Changes** or **Undo Changes** to close the edit mode.

Table continues…

Icon	Name	Description
	Undo Changes	Returns you to the non-edit mode of the dashboard without applying changes.
	Change Layout	Lets you select a different layout for the widgets on the dashboard.
	Add New Widget	Lets you search for and add a new widget to the dashboard.
	Apply Changes	Applies and saves all of the changes.

Home dashboard configuration

Use the following procedures to configure the Home dashboard. Click the product name on the menu bar to go to the Home dashboard from any other page in the interface.

Changing the layout of the dashboard

When you log on to the system for the first time, the Home page displays the dashboard with the default widgets on a default layout. You can change the layout to suit your needs.

About this task

Use this procedure to change the layout of the dashboard.

Procedure

1. On the dashboard, click **Customize Dashboard**.

2. In the dashboard edit mode, click **Change Layout**.

3. In the Edit Dashboard dialog box, select the layout for the dashboard.

4. Click **Close**.

   The system displays the dashboard in the new layout.

5. To save the layout, click **Apply Changes**.

Adding a widget

About this task

Use this procedure to add a widget to the dashboard. The widgets available to add depend on what widgets are currently on your dashboard, your product, and licensing.

Procedure

1. On the dashboard, click **Customize Dashboard**.

2. In the dashboard edit mode, click **Add New Widget**.

3. In the Add new widget dialog box, select the widget that you want to add from the available widgets.

   The system adds the widget to the dashboard ahead of the existing widgets on the dashboard.

4. To save the change, click **Apply Changes**.

Removing a widget

About this task

Use this procedure to remove a widget from the dashboard.

Procedure

1. On the dashboard, click **Customize Dashboard**.

2. In the dashboard edit mode, go to the widget that you want to remove.

3. From the widget toolbar, click **remove widget**.

   The system removes the widget from the dashboard.

4. To save the change, click **Apply Changes**.

Changing the location of a widget

About this task

Use this procedure to drag and drop a widget to a different location on the dashboard.

Procedure

1. On the dashboard, click **Customize Dashboard**.

2. In the dashboard edit mode, go to the widget that you want to move.

3. From the widget toolbar, click and hold **change widget location** while you drag and drop the widget to a new location on the dashboard.

4. To save the change, click **Apply Changes**.

Configuring the widget refresh interval

About this task

Use this procedure to configure the widget refresh interval for a widget. You can disable the widget refresh interval or schedule a refresh at regular intervals. The default is disable.

Procedure

1. On the dashboard, click **Customize Dashboard**.

2. In the dashboard edit mode, go to the widget for which you want to configure the widget refresh interval.

3. From the widget toolbar, click **Configure Widget**.

4. In the **Widget Refresh Interval** field, select the interval from the drop-down list.

5. Click **Apply**.

6. To save the changes to the dashboard, click **Apply Changes**.

Configuring the backup schedule summary

Use this procedure to configure how to display a summary of the device count by schedule interval for the device backup feature.

Before you begin

Make sure that the Backup Schedule Summary was added to the dashboard.

Procedure

1. On the dashboard, click **Customize Dashboard**.

2. In the dashboard edit mode, go to the Backup Schedule Summary widget.

3. From the widget toolbar, click **edit widget configuration**.

4. On the Device Backup Schedule Summary edit page, do the following:

   a. Disable or select a **Widget Refresh Interval**.

   b. Select an **Interval Unit**.

   c. Select an **Interval Range**.

   d. Select the **Number of Interval Ranges**.

   e. Select whether to **Show Active Schedules Only**.

5. Click **Apply**.

6. To save the changes to the dashboard, click **Apply Changes**.

Backup Schedule Summary field descriptions

Use the data in this table to understand the backup schedule summary.

Field	Description
Widget Refresh Interval	Disable the widget refresh interval or schedule a refresh at regular intervals. Values are Disable (default), 30 secs, 60 secs, 120 secs, and 300 secs.
Interval Unit	Specify a unit for the interval range. Values are Minutes, Hours, Days (default), or Weeks.
Interval Range	Specify the size of the interval range. Values are 1 (default) through 10.
Number of Interval Ranges	Specify how many interval ranges to display. Values are 1 (default) through 10.
Show Active Schedules Only	Values are True (default) and False.

Chapter 6: 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 the system.

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.

Security settings

The system provides a way to customize logon banner that appears after a user logs on. The customizable banner is intended for use by customers who have security policies that require network equipment to display a specific message to users when the users log on.

Customized interface

The system provides the feature to add a logo to the web interface. Organizations can customize the logo without removing the Avaya logo.

Single sign-on cookie domain

Single sign-on (SSO) allows access to multiple software systems that are related but independent from each other. SSO allows you to log in with a single ID and password to access many different software systems without having to use different usernames and passwords.

The single sign-on cookie domain allows a particular domain for all of the software systems.

When you configure the primary and backup security severs in different domains, Single Sign-on (SSO) requires authentication to switch from the primary to backup security server. For authentication, the primary and backup server domain names must match.

Password and security policies procedures

Viewing security policies

Perform this procedure to view the security policies.

Before you begin

Ensure that you are logged on as an administrator.

About this task

You can also access security policies through **Administration** > **System Management** > **Administrators** > **Policies**.

Procedure

1. Select **Administration** > **Policies**.

2. View the Policies configuration options.

Editing password policies

Edit password policies including aging, history, strength, and lockout password policies.

Before you begin

Ensure that you are logged on as an administrator.

About this task

You can also access security policies through **Administration** > **System Management** > **Administrators** > **Policies**.

Procedure

1. Select **Administration** > **Policies**.

2. In the Password Policy (for locally authenticated users) section, click **Edit**.

3. On the Password Policy page, to enforce password aging policies, select the **Aging** check box and configure the aging policy.

4. To enforce a policy against previously used passwords, select the **History** check box and configure the history policy.

5. To enforce password content standards, select the **Strength** check box and configure the strength policy.

6. To enforce the lockout of a user after failed login attempts, select the **Lockout** check box and configure the lockout policy.

7. Click **Save**.

Password policy field descriptions

Name	Description
Aging	If selected, enforces the password aging policies.
Enable expired password change	If selected, allows the changing of an expired password.

Table continues…

Name	Description
Expiration period	The number of days before a password expires. Range is 2 to 365 days.
Expiration warning	The number of days before the system displays an warning message during login that the password is about to expire. Range is 1 to 15 days.
Minimum age	The number of days before a password can be changed after the last changes. Range is 0 to 7 days. A minimum age prevents password recycling that could defeat the history policy.
History	If selected, enforces the history policy against previously used passwords.
Previous passwords blocked	The number of previously used passwords that are blocked from being reused. Range is 1 to 99.
Strength	If selected, enforces the strength policy for the content of a password including the following requirements: • Passwords cannot have a character repeated more than twice consecutively. • Passwords cannot have the login name of the user, either in forward of reverse.
Minimum total length	The minimum number of total characters for the password. Range is 6 to 25 characters.
Minimum by character type	The minimum number of characters required of a certain type. The sum cannot exceed the minimum total length. A value of 0 indicates that the character type is not required. • Lower case—The minimum number of lowercase characters required in the password. The default value is 1. • Upper case—The minimum number of uppercase characters required in the password. The default value is 1. • Numeric case—The minimum number of numeric characters required in the password. The default value is 1. • Special case—The minimum number of special characters required in the password. The default value is 1.
Lockout	If selected, enforces the user lockout policy after failed login attempts.

Table continues…

Administration using Avaya Fabric Orchestrator

Name	Description
Consecutive Invalid Login Attempts	The number of failed consecutive login attempts before the user is locked out. Range is 1 to 20 attempts. The default is 5.
Interval for Consecutive Invalid Login Attempts	The number of minutes of failed consecutive login attempts before the user is locked out. Range is 0 to 120 minutes.
Lockout Time	The number of minutes until the account is unlocked. Range is 0 to 120 minutes.

Editing session properties

Perform this procedure to manage the properties of user sessions including maximum session time and maximum idle time. Saved modifications only apply to newly logged in users.

Before you begin

Ensure that you are logged on as an administrator.

About this task

You can also access security policies through **Administration** > **System Management** > **Administrators** > **Policies**.

Procedure

1. Select **Administration** > **Policies**.

2. In the Session Properties section, click **Edit** to open the Session Properties page.

3. In the **Maximum Session Time** field, enter a number for the maximum session time in minutes from 10 to 1440.

4. In the **Maximum Idle Time** field, enter a number for the maximum idle time in minutes from 10 to 1440.

   🛑 **Important:**

   The maximum idle time must not exceed the maximum session time.

5. Click **Save**.

Variable Definitions

Variable	Value
Maximum Session Time	Number for maximum session time in minutes from 10 to 1440. The default value is 120.
Maximum Idle Time	Number for the maximum idle time in minutes from 10 to 1440. The default value is 30.

Table continues…

Variable	Value
	⊛ **Note:** • The maximum idle time must not exceed the maximum session time.

Editing login warning banner

Perform this procedure to customize the message for the login warning banner.

Before you begin

Ensure that you are logged on as an administrator.

About this task

You can also access security policies through **Administration** > **System Management** > **Administrators** > **Policies**.

Procedure

1. Select **Administration** > **Policies**.

2. In the Security Settings section, click **Edit** to open the Security Settings page.

3. In the **Login Warning Banner** text area, edit the text as required.

   The maximum number of characters allowed is 2500.

4. Click **Save**.

Security Settings field descriptions

Field	Description
Login Warning Banner	Specifies the text for the Login Warning Banner.

Adding a customized image

Add a customized image to the interface.

The supported image file formats are PNG, GIF, and JPEG. The supported image dimensions are 100x51 px.

Before you begin

Ensure that you are logged on as an administrator.

About this task

You can also access security policies through **Administration** > **System Management** > **Administrators** > **Policies**.

Procedure

1. Select **Administration** > **Policies**.

2. In the Customized Interface section, click **Edit**.

3. On the Customized Interface page, click **Browse** and select a file to upload.

4. To change the image ALT attribute, enter the text you want to display in the **Image Alt Attribute** field.

5. Click **Save**.

Customized interface field descriptions

Name	Description
Upload File	Specifies the file you want to upload.
Change Image ALT Attribute	Specifies the alternate text for the image that you uploaded.

Editing the Single Sign-on Cookie Domain

Perform this procedure to change the Single Sign-on Cookie Domain.

When you configure the primary and backup security servers in different domains, Single Sign-on (SSO) requires authentication to switch from the primary to backup security server. For authentication, the primary and backup security server domain names must match.

Before you begin

Ensure that you are logged on as an administrator.

About this task

You can also access security policies through **Administration** > **System Management** > **Administrators** > **Policies**.

Procedure

1. Select **Administration** > **Policies**.

2. In the Single Sign-on Cookie Domain section, click **Edit** to open the Edit Domain Name page.

3. From the **Single Sign-On Cookie Domain** list, select a URL to change the Single Sign-on Cookie Domain.

4. Click **Save**.

   Important:

   After you change the SSO Cookie Domain, users must clear the existing related cookies from the cache in the Internet browser for all users.

Single sign-on cookie domain field descriptions

Name	Description
Single Sign-on Cookie Domain	Specifies the SSO cookie domain name.

Chapter 7: User management and Role Based Access Control

Managing roles

You can perform various Role Based Access Control (RBAC) tasks required to manage roles within the system. You can add or delete a role name, provide group-level authentication functions and element permissions.

Perform role management tasks in **Administration** > **Roles**.

Role Based Access Control

You require appropriate permissions to perform any task. The administrator grants permissions to users by assigning appropriate roles. The Role Based Access Control (RBAC) 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 the system 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 the system has 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)

Table continues…

Role Name	Element Mapping	Role Permission Assigned
	AFO Configuration Services	Modify for all managers
	AFO Administrative 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 Administrative Services	Access AFO maintenance services
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

About this task

You can also access role information through **Administration** > **System Management** > **Administrators** > **Security** > **Roles**.

Procedure

1. Select **Security** > **Roles**.

2. Expand the **System Administrator** folder.

3. Click **AFO Network Administrator**, and then click **New**.

4. On the Add New Role page, fill in the **Role Name** and **Role Description** fields.

5. Click **Commit and Continue**.

   The system displays the Role Details page.

6. To select element or network service, or both, to map to a created role, click **Add Mapping**.

7. In the Element or Resource Type field, select **AFO Primary Roles**.

8. In the Element or Resource Instance field, select **All**.

9. Click **Next**.

10. Select the check box for **Select/Unselect All**, and then click **Commit**.

    • If you have migrated data from a previous version or legacy product, check the ReadWrite check boxes for the managers you want to assign to the existing user.

11. To select element or network service, or both, to map to a created role, click **Add Mapping**.

    • If the user already exists due to data migration from a previous release version or legacy product, skip this step.

12. Click **Commit**.

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

13. 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.
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

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

⊛ **Note:**

Predefined or system-defined roles cannot be modified.

About this task

You can also access role information through **Administration** > **System Management** > **Administrators** > **Security** > **Roles**.

Procedure

1. Select **Security** > **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.
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.

Icons	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

About this task

You can also access role information through **Administration** > **System Management** > **Administrators** > **Security** > **Roles**.

Procedure

1. Select **Security** > **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 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 the system. • External- Users stored in the directory server of the customer.

Icons	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

About this task

You can also access role information through **Administration** > **System Management** > **Administrators** > **Security** > **Roles**.

Procedure

1. Select **Security** > **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 to unassign.

6. Click **Commit**.

Copying permission mapping for a role

About this task

You can also access role information through **Administration** > **System Management** > **Administrators** > **Security** > **Roles**.

Procedure

1. Select **Security** > **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**.

5. On the Copy User Assignment page, 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**.

7. On the Role Details page, click **Commit**.

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

Editing a custom role

About this task

You can also access role information through **Administration** > **System Management** > **Administrators** > **Security** > **Roles**.

Procedure

1. Select **Security** > **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. 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 37.

5. 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, _.
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

About this task

You can also access role information through **Administration** > **System Management** > **Administrators** > **Security** > **Roles**.

Procedure

1. Select **Security** > **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

The administrator performs the user management tasks required to manage users within the system.

Viewing existing users

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

About this task

You can also access user information through **Administration** > **System Management** > **Administrators** > **Administrative Users**.

Before you begin

Ensure that you are logged on as an administrator.

Procedure

1. Select **Administration** > **Users**.

    The Administrative Users page lists users configured for access to the system.

2. View the information for existing users.

Adding a new local or external user

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

About this task

You can also access user information through **Administration** > **System Management** > **Administrators** > **Administrative Users**.

Before you begin

Ensure that you are logged on as an administrator.

Procedure

1. Select **Administration** > **Users**.

2. On the Administrative Users page, click **Add**.

3. On the Add New Administrative User page, in the **User ID** field, enter the user ID.

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

   • Local

   • External

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

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

   > **Important:**
   >
   > The password that you enter for the new local user is temporary. When a new user logs on to the system for the first time, the system requires the user to change this password. Avaya recommends that users record the new password in a secure place.

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

8. On the Add New Administrative User Step 2 page, in the **Role Name** column, select the Role Name check boxes that you want to assign to the user, and 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 _.
Authentication type	Type of user: Local user or External user.
Full Name	Full name of the user.

Table continues…

Field	Description
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.

Disabling a user

Perform this procedure to disable a user.

About this task

You can also access user information through **Administration** > **System Management** > **Administrators** > **Administrative Users**.

Before you begin

- Ensure that you are logged on as an administrator.

Procedure

1. Select **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

Perform this procedure to delete a user.

About this task

You can also access user information through **Administration** > **System Management** > **Administrators** > **Administrative Users**.

Before you begin

- Ensure that you are logged on as an administrator.

Procedure

1. Select **Administration** > **Users**.

2. Under **User ID**, select the User ID check box that you want to delete, and then click **Delete**.

3. On the Delete Users page, you are prompted to confirm the deletion of the user. Click **Delete**.

❗ Important:

> Users cannot delete their own account.

Configuring user properties

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

About this task

You can also access user information through **Administration** > **System Management** > **Administrators** > **Administrative Users**.

Before you begin

- Ensure that you are logged on as an administrator.

Procedure

1. Select **Administration** > **Users**.

2. On the Administrative Users page, under **User ID**, click the User ID for 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 button.

4. In the Password Reset section, in the **Password** field, enter a new password.

5. In 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 Reset:	
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.

Table continues…

Field	Description
Authentication type	
Local	The user is authenticated by the default Open LDAP service.
External	The user is authenticated by the external authentication service if the service 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

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

Before you begin

- Ensure that you are logged on as an administrator.

About this task

You can also access user information through **Administration** > **System Management** > **Administrators** > **Administrative Users**.

Procedure

1. Select **Administration** > **Users**.

2. On the Administrative Users page, under **User ID**, click the User ID for which you want to set properties and assign roles.

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

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

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

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

5. On the User Details page, click **Commit**.

External authentication scheme and authentication server configuration

The External Identity Repositories web page in System Manager contains a summary page for authentication scheme and authentication servers. You can configure the authentication scheme and the authentication servers for System Manager.

The system 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.

The authentication scheme policy determines the order in which you can use the authentication authorities. The supported order is as follows:

1. Local users (default)
2. External RADIUS users then local users
3. External LDAP users then local users
4. External LDAP users, then external RADIUS users, then local users
5. External RADIUS users, then external LDAP users, then local users
6. External KERBEROS server

Editing the authentication scheme

About this task

Perform this procedure to edit the authentication scheme.

Before you begin

Ensure that you are logged on as an administrator.

Procedure

1. Select **Administration** > **System Management**.

   The system launches the SMGR page in a separate browser.

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

3. On the External Identity Repositories, in the **Authentication Scheme** section, click **Edit**.

4. On the Authentication Scheme page, select the required authentication scheme, and then click **Save**.

> ⊛ **Note:**
>
> If Authentication Servers is undefined, only the Local users Authentication Scheme is available.

Configuring authentication servers

Perform this procedure to configure the 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 servers.

> ⊛ **Note:**
>
> Repeat the procedure to configure **Provision Second LDAP Server**.

Before you begin

- Ensure that you are logged on 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. Select **Administration** > **System Management**.

   The system launches the SMGR page in a separate browser.

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

3. On the External Identity Repositories page, in the **Authentication Servers** section, click **Configure**.

4. On the Authentication Servers page, 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**.

Provision LDAP Server field descriptions

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	The distinguished name for the root binding. For example, type cn for Users.
Password for Root Binding	The password for the root binding in this field.

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 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. Select **Administration** > **System Management**.

   The system launches the SMGR page in a separate browser.

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

3. On the External Identity Repositories page, in the **Authentication Servers** section, click **Configure**.

4. On the Authentication Servers page, 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.

Radius Server field descriptions

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.

Provisioning the Kerberos server

About this task

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

Before you begin

- If you use Firefox to gain access to the system, 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 the system.
- Log on to the system as admin.

Procedure

1. Select **Administration** > **System Management**.

   The system launches the SMGR page in a separate browser.

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

3. On the External Identity Repositories page, in the **Authentication Servers** section, click **Configure**.

4. On the Authentication Servers page, 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**: Browse to and choose the Kerberos server key file.

5. Click **Save**.

> **⓵ 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 the system using the Logout link. Close the Web browser to exit the application.

Kerberos Server field descriptions

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.

Provisioning SAML Remote Identity Provider

About this task

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

Procedure

1. Select **Administration** > **System Management**.

   The system launches the SMGR page in a separate browser.

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

3. On the External Identity Repositories page, in the **Authentication Servers** section, click **Configure**.

4. On the Authentication Servers page, 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**: Browse to and choose the metadata file.

5. Click **Save**.

Provision SAML Remote Identity Provider field descriptions

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.

Provisioning User Certificate Authentication

About this task

Perform this procedure to assign the user certificate authentication

Procedure

1. Select **Administration** > **System Management**.

   The system launches the SMGR page in a separate browser.

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

3. On the External Identity Repositories page, in the **Authentication Servers** section, click **Configure**.

4. On the Authentication Servers page, in the **User Certificate Access Level** field, select the user certificate access level from the list.

5. Click **Save**.

Configuring SAML

The system is automatically configured as a Hosted Service Provider during installation or upgrade. 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 from the **System Management** page.

Editing SAML Hosted Service Provider properties

About this task

Perform this procedure to modify the configuration.

Procedure

1. Select **Administration** > **System Management**.

   The system launches the SMGR page in a separate browser.

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

3. On the SAML Configuration page, 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 the system.

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

5. Click **Save**.

Chapter 8: Preference management

Managing preferences

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

From the web interface, click the Preferences icon from the quick access toolbar to open the Preferences page. The Preferences navigation pane is on the left side of the page.

The root level items of the Preferences navigation pane are:

- Global
- Configuration
- Monitoring
- IP Flow
- Virtualization
- MSC

Configuring Global Preferences

Use Global Preferences to manage preferences used by multiple services across the system.

✱ **Note:**

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

The Global Preferences page displays the SNMP and email preferences on the right side of the page and displays a navigation pane on the left side of the page.

About this task

Perform this procedure to configure the SNMP and email preferences for multiple services simultaneously and to avoid configuring these preferences in multiple locations.

Make sure that the SMTP host is accessible from the configuration virtual machine (VM). You can use the ping command to test if the SMTP host is reachable from the configuration VM. If not, you should update the /etc/hosts in the configuration VM about the SMTP host FQDN and IP address.

Procedure

1. Select the **Preferences** icon from the quick access tool bar 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 the **Retries** and **Timeout** 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** check box.

      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 Backup SMTP **Host, User Name, Password, From, and Port** fields.

   b. Select or clear the **Use SSL** check box.

5. In the Primary host (vCenter or ESXi server) Information section:

   a. Enter the primary 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.

   d. To test the connectivity to the primary host, click **Validate Connection**.

      The system displays the validation message.

6. Click **Apply**.

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
Primary SMTP	
Host	Specifies the primary host that the system 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).

Table continues…

Field	Description
Password	Specifies the primary password that permits the system 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 primary SNMP port number.
Use SSL	Specifies the secure socket layer connection. Select the check box for secure connection.
Backup SMTP	
Host	Specifies the backup host that the system uses to set up a connection to the corporate e-mail server.
User Name	Specifies the backup SMTP user name (example: john.doe@avaya.com).
Password	Specifies the backup password that permits the system 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.
Primary Host (vCenter or ESXi server) Information	
Hostname/IP Address	Specifies the primary Hostname or IP Address
Username	Specifies the primary host User name.
Password	Specifies the primary host

Configuring Configuration preferences

Use the following procedures to configure general server and logging preferences.

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 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 procedures to configure logging.

Configuring Audit Log logging

About this task

Perform the following procedure for configuring audit log logging.

Procedure

1. Select the **Preferences** icon from the quick access toolbar to open the Preferences page.

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

3. Click the **Logging** tab.

4. 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.

5. Click **Archive**.

6. In the confirmation dialog box, click **Apply**.

Configuring Debug Log logging

About this task

Perform the following procedure to configure debug log logging.

Before you begin

You must configure the audit log. For more information, see Configuring Audit Log logging on page 57.

Procedure

1. Select the **Preferences** icon from the quick access toolbar to open the Preferences page.

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

3. Click the **Logging** tab.

4. 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.

5. Click **Apply**.

   * **Note:**

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

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.

Click the **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.

3. On the Monitoring Preferences page, perform the following tasks in the Syslog Settings section:

   - Set the **Maximum age**.

   - Enter the **Maximum number**.

   - Set the **Limit to disc. devices** to true or false.

   - Enter the **Listener port**.

   - Enter the **Archive depth**.

   - Enter information in the **Archive directory** field.

   - Enter information in the **Forwarding** section.

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

Syslog Viewer Settings field descriptions

Use the data in the following table to understand the Syslog Viewer Settings.

Name	Description
Maximum age	Specifies the maximum age. Entries that are older than the maximum age defined in this field are purged from the database.
	The default is 7 days.
Maximum number	Specifies the maximum number. After the maximum number of entries are in the database, the oldest entries are deleted as new entries are added.
	The default is 1,000,000.
Limit to disc. devices	Specifies the limit to discovery devices. This determines whether the trap data is limited to discovered devices.
	The default is false.
Listener port	Specifies the listener port.
	The default is 514.
Archive depth	Specifies the archive depth. Older files beyond this number are deleted.
	The default is 10.
Archive directory	Specifies the archive directory. Enter the file path for the directory where you want archive files to be stored.

Table continues…

Name	Description
	The default is notificationArchive.
Forwarding	Specifies forwarding information. Click **Add Forwarder** to enter the Host Address and port number for syslog information.

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.

3. On the Monitoring Preferences page, perform the following tasks in the Trap Settings section:

   • Set the **Maximum age**.

   • Enter the **Maximum number**.

   • Set the **Limit to disc. devices** to true or false.

   • Set the **Limit to auth. devices** to true or false.

   • Enter the **Archive depth**.

   • Enter the **Listener port**.

   • Enter the **Archive directory** field information.

   • Enter the **Forwarding** field information.

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

Traps settings field descriptions

Use the data in the following table to understand the Traps settings.

Name	Description
Maximum age	Specifies the maximum age. Entries that are older than the maximum age defined in this field are purged from the database. The default is 7 days.
Maximum number	Specifies the maximum number. After the maximum number of entries are in the database, the oldest entries are deleted as new entries are added. The default is 1,000,000.

Table continues…

Name	Description
Limit to disc. devices	Specifies the limit to disc. devices. This determines whether the trap data is limited to discovered devices. The default is false.
Limit to auth. devices	Specifies the limit to auth. devices. This determines whether the trap data is limited to authenticated devices. The default is false.
Archive depth	Specifies the archive depth. Older files beyond this number are deleted. The default is 10.
Listener port	Specifies the listener port. The default is 162.
Archive directory	Specifies the archive directory. Enter the file path for the directory where you want archive files to be stored. The default is notificationArchive.
Forwarding	Specifies forwarding information. Click **Add Forwarder** to enter the destination IP address for trap information.

Configuring IP Flow management preferences

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

Select the **Preferences** icon from the quick access toolbar to open the Preferences page.

Configuring collector information

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

- UDP ports for collecting data — 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 — 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 — 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 IP Flow sends a collector E-mail notification when IPFIX data exceeds the license limit.

Next steps

Perform the procedure for

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

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 4320. For hours, enter a value between 1h and 72h

Choice Option	Choice Description
Minutes	Enter a positive value between 1 and 4320 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 63.

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 61.
- Capture duration. For more information, see Configuring the capture duration and look back time on page 62.

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 `Default` 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.

Virtualization Preferences

Configuring Virtualization Preferences

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

Click the **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.

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, 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.

Choice Option	Choice Description
Core Device	If the check box is selected, 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 the Inventory Audit Setting

About this task

Perform the following steps to configure the Inventory Audit Setting.

Procedure

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

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

2. Click the **General** tab.

3. In the Inventory Audit Setting section, select or clear **Refetch Virtual Mac Address from Hosts** field.

   ✳ **Note:**

   This field is selected by default.

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 the system for the first time through the 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 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.

Configuring 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 Scheduler settings

You can configure settings for Hypervisor Connectivity, Monitor Purge, and Audit Log Purge jobs.

Rescheduling Hypervisor Connectivity jobs

About this task

Perform the following steps to reschedule Hypervisor Connectivity jobs.

⊛ **Note:**

Each time the Virtualization application starts and the 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 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**.

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. Click the 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

Accessing MSC preferences

Use MSC preferences to configure preferences related to the Management Server Console, Product Licensing and Delivery System (PLDS), and Software Library. This section provides information about launching and configuring Management Server Console (MSC) preferences.

After you configure PLDS settings, the system downloads upgrades and software bundles for future installation.

Procedure

1. To access MSC Preferences, do the following:

   a. Click the **Preferences** icon on the quick access toolbar on the top right.

   b. On the Preferences page, click **MSC** on the left navigation pane to open the MSC preferences page.

   OR

2. To access MSC Preferences from the Solution Software Director page, do the following:

   a. On the menu bar, select **Administration** > **Solution Software Director**.

   b. On the Solution Software Director page, click the **MSC Preferences** icon from the top left toolbar to open the 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. You can store the customer Avaya PLDS user ID and password in this location.

Procedure

1. To access MSC Preferences, do the following:

   a. Click the **Preferences** icon on the quick access toolbar on the top right.

   b. On the Preferences page, click **MSC** from the left navigation pane.

   OR

2. To access MSC Preferences from the Solution Software Director (SSD) page, do the following:

   a. On the menu bar, select **Administration** > **Solution Software Director**.

   b. Click the **MSC Preferences** icon from the top left toolbar.

3. On the MSC preferences page, click the **PLDS** tab.

4. In 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.

5. Select the **Use Proxy** check box and enter the `proxy IP address` in **Proxy IP** and select a **Port**, to configure the proxy server details.

6. Click **Apply** to save.

Configuring External Storage settings

Use this procedure to configure external storage settings for backup, upgrade, and logging tasks. You can configure the following protocols for transferring files:

• Secure Copy Protocol (SCP)

• File Transfer Protocol (FTP)

Procedure

1. To access MSC Preferences, do the following:

   a. Click the **Preferences** icon on the quick access toolbar on the top right.

   b. On the Preferences page, click **MSC** from the left navigation pane.

OR

2. To access MSC Preferences from the Solution Software Director (SSD) page, do the following:

   a. On the menu bar, select **Administration** > **Solution Software Director**.

   b. Click the **MSC Preferences** icon from the top left toolbar.

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

4. 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.

5. 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.

6. Click **Apply**.

Configuring Backup settings

The system 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 system, perform a backup of the application related data, common services, and platform data. If an error occurs, use backup configuration files to return the system to a previous state.

Avaya recommends that you keep several copies of backup files.

Procedure

1. To access MSC Preferences, do the following:

   a. Click the **Preferences** icon on the quick access toolbar on the top right.

   b. On the Preferences page, click **MSC** from the left navigation pane.

   OR

2. To access MSC Preferences from the Solution Software Director (SSD) page, do the following:

   a. On the menu bar, select **Administration** > **Solution Software Director**.

   b. Click the **MSC Preferences** icon from the top left toolbar.

3. On the MSC Preferences page, click the **Backup** tab.

4. 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).

5. Enter the `backup directory path` in the **Backup directory** field.

6. In the **Backup Purge** section select the backup archive files purge threshold in MB from the drop-down menu.

7. In the **Backup Scheduler** section, select one of the options:

Choice Option	Choice Description
Every Month On:	Select a date to schedule backup on a monthly basis.
Every Week On:	Select a day to schedule backup on a weekly basis.
Everyday At:	Select a time to schedule backup on a daily basis.

8. 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.

Procedure

1. To access MSC Preferences, do the following:

    a. Click the **Preferences** icon on the quick access toolbar on the top right.

    b. On the Preferences page, click **MSC** from the left navigation pane.

    OR

2. To access MSC Preferences from the Solution Software Director (SSD) page, do the following:

    a. On the menu bar, select **Administration** > **Solution Software Director**.

    b. Click the **MSC Preferences** icon from the top left toolbar.

3. On the MSC Preferences page, click the **Logging** tab.

4. In 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).

5. In the **External Syslog Server** section:

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

6. In the **Log Purge** section:

   • Select a retention limit threshold value in MB for the log archive files.

7. In 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.

8. Click **Apply**.

Chapter 9: EDM

Enterprise Device Manager

The following chapter contains conceptual and configuration information for Enterprise Device Manager (EDM).

Plugins inventory

The EDM plugin is a device plugin for a device version, or type, that you can install on the platform. You can install plugins on a base or advanced license. The network administrator and SMGR system administrator can perform the plugin management. To install, uninstall, or view the EDM plugin, access the plugins inventory, from the navigation pane, under **Administration** > **Device Plug-in Management**.

The platform displays the EDM Plugin Inventory with a table containing all the installed plugins on the 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. If you want to perform QoS / Filters operation on a particular device, 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 you launch EDM on a device for which the software version is not compatible, the system displays an EDM plugin version mismatch window.

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-right 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.
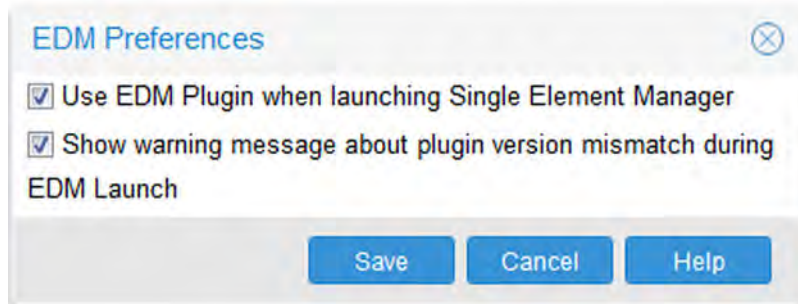
> **! Important:**
>
> If you clear the **Use EDM Plugin when launching Single Element Manager** check box, the device may have performance issues.

Downloading EDM plugin

Perform the following procedure to download an EDM plugin from the Avaya support site.

Procedure

1. Open a web browser, and go to the Avaya support website: https://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 to your computer.

Installing EDM plugin

Perform the following procedure to install an EDM plugin on the platform.

Before you begin

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

Procedure

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

4. To select the EDM Plugin file, click **Browse**.

5. Browse to the EDM plugin file, and then click **Open**.

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.

The system looks up the device inventory and then locates the corresponding EDM plugin in the repository.

Before you begin

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

Before you begin

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

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 Plugin**, which is the minus sign on the top-left toolbar.

4. Click **Yes**.

   If the uninstall is successful, the platform displays the following message: EDM pluging uninstall successful. If the uninstall is not successful, the platform 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 to look up the device inventory, and then locate any unused EDM plugins.

Before you begin

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

Procedure

1. 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, the system displays `Plugins uninstall successful.`

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

Refreshing the plugin inventory table

Perform the following procedure to refresh the plugin inventory table.

Before you begin

- You must have system administrator or network administrator role rights to access the Plugins Inventory.
- Ensure you log on to the platform as an administrator.

Procedure

1. Download the **EDM plugin**.

2. From the navigation pane, select **Administration** > **Device Plug-in Management**.

3. From the toolbar, click **Refresh Plugin Inventory**.

Chapter 10: 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.

You must be logged into the system, and launch vEDM from the 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 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.

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

- Ensure that you log on as an administrator.

Procedure

Select **Administration** > **vEDM** to start **vEDM**.

The Device Logical View displays.
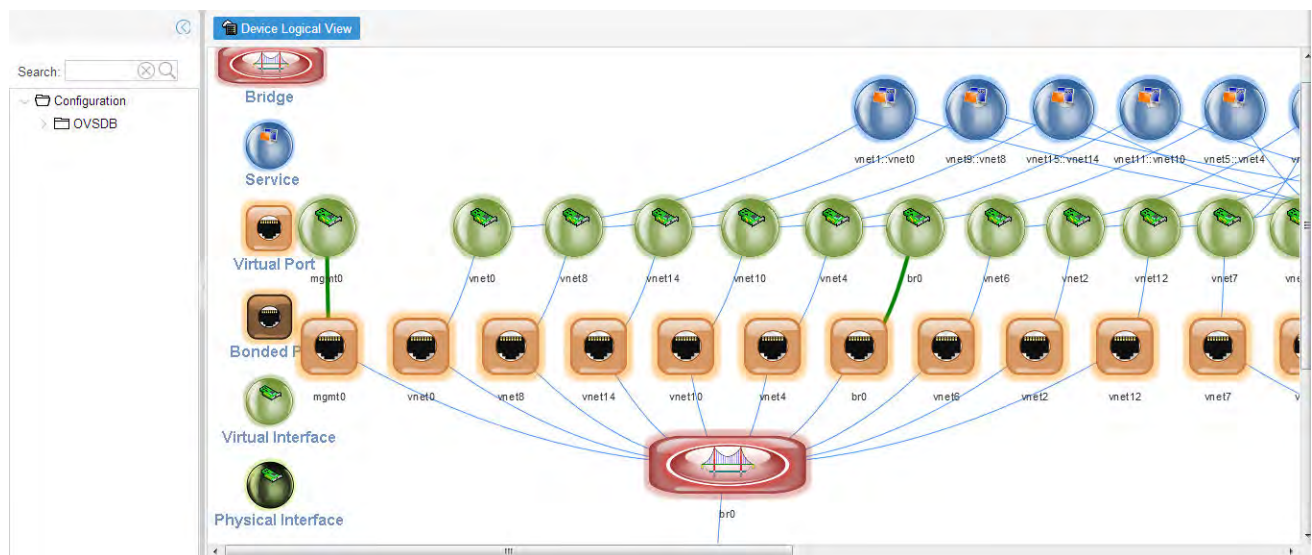
vEDM field descriptions

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.

Table continues…

Name	Description
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

- Ensure that you log on as an administrator.

Procedure

1. Select **Administration** > **vEDM** to start **vEDM**.

2. Select **Configuration** > **OVSDB** > **Open-vSwitch**.

3. Select the **OVSDB** tab to view Open Virtual Switch Database information.
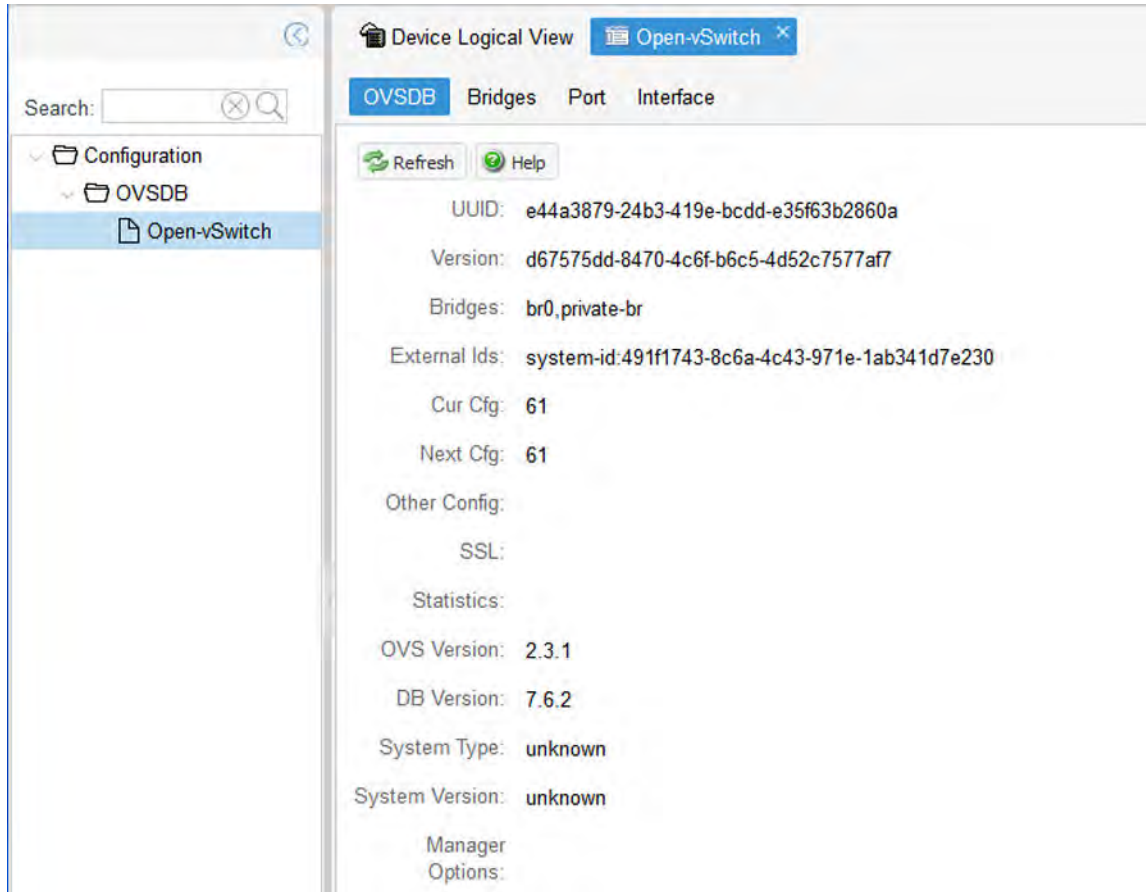
OVSDB tab field descriptions

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

• Ensure that you log on as an administrator.

Procedure

1. Select **Administration** > **vEDM** to start **vEDM**.

2. Select **Configuration** > **OVSDB** > **Open-vSwitch**.

3. Select the **Bridges** tab.
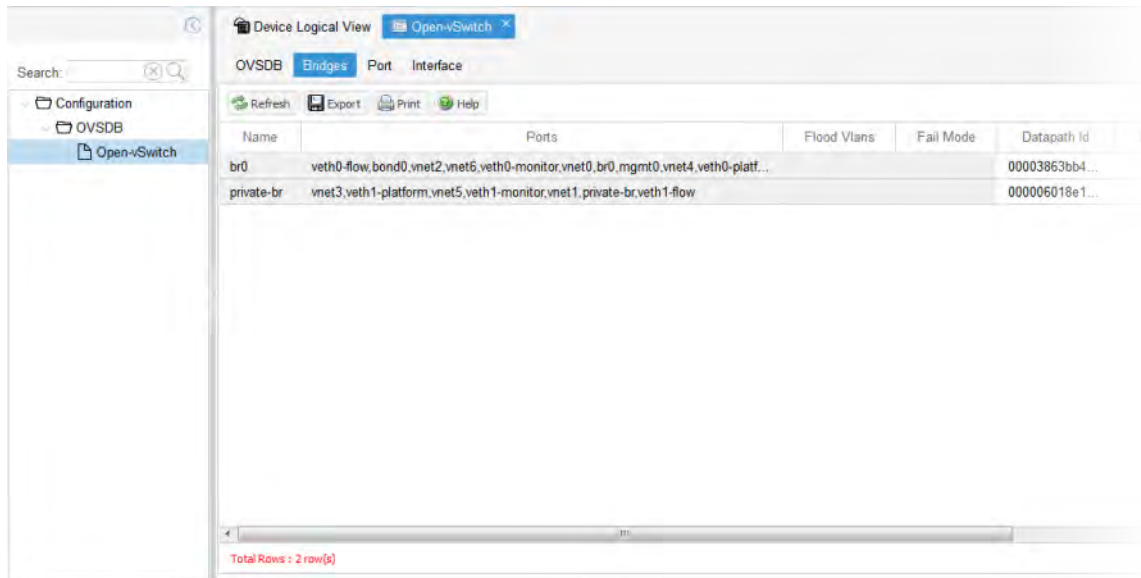
4. **(Optional)** To refresh the table, click **Refresh**.

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

• Ensure that you log on as an administrator.

Procedure

1. Select **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

• Ensure that you log on as an administrator.

Procedure

1. Select **Administration** > **vEDM** to start **vEDM**.

2. Select **Configuration** > **OVSDB** > **Open-vSwitch**.

3. Select the **Port** tab.
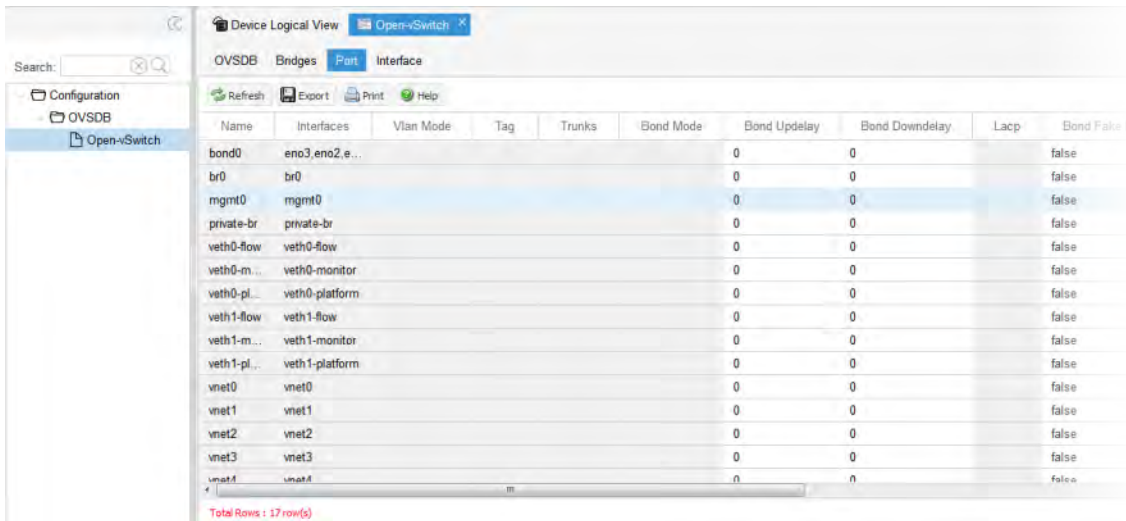
4. **(Optional)** To refresh the table, click **Refresh**.

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 • native-tagged • native-untagged

Table continues…

Name	Description
	• 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.
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.

Table continues…

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

Administration using Avaya Fabric Orchestrator

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

• Ensure that you log on as an administrator.

Procedure

1. Select **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. 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

• Ensure that you log on as an administrator.

Procedure

1. Select **Administration** > **vEDM** to start **vEDM**.

2. Select **Configuration** > **OVSDB** > **Open-vSwitch**.

3. Select the **Interface** tab.
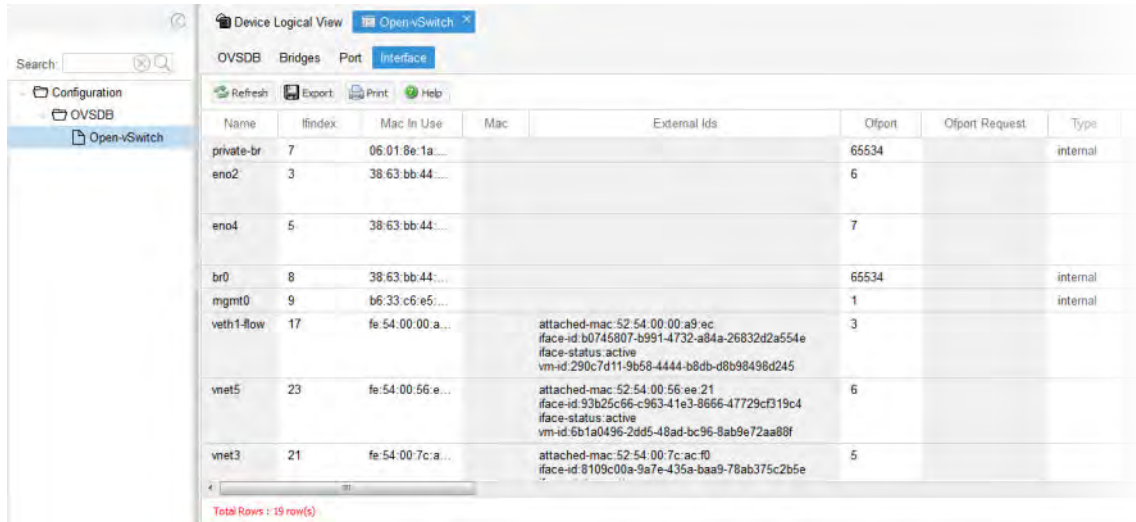
4. **(Optional)** To refresh the table, click **Refresh**.

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

- Ensure that you log on as an administrator.

Procedure

1. Select **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. To print the **Interface** tab information, click **Print**.
7. Select the printer name where you want the information to print.

8. Click **OK**.

Chapter 11: Appliance Device Manager (ADM)

This chapter provides concepts and procedures to configure Appliance Device Manager (ADM).

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 appliance and co-resides within the Kernal Virtual Machine (KVM). ADM manages the appliance and the services (virtual machines) present in the appliance. You can access ADM using one of the following supported Web browsers:

- Microsoft Internet Explorer, version 11
- Mozilla FireFox, versions 47, and later
- Safari (macOS v10.8 Mountain Lion, and later)

To configure multiple devices through one interface, you can install your system on a remote server.

The ADM feature enables you to:

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

* **Note:**

You can also access ADM when the platform service is down, using the local login. For more information, see Access to ADM when platform service is down on page 106.

ADM Window

The ADM window displays the overall health and status of the appliance. Use the ADM window to identify and troubleshoot issues. The following figure and table show the different sections of the ADM window:
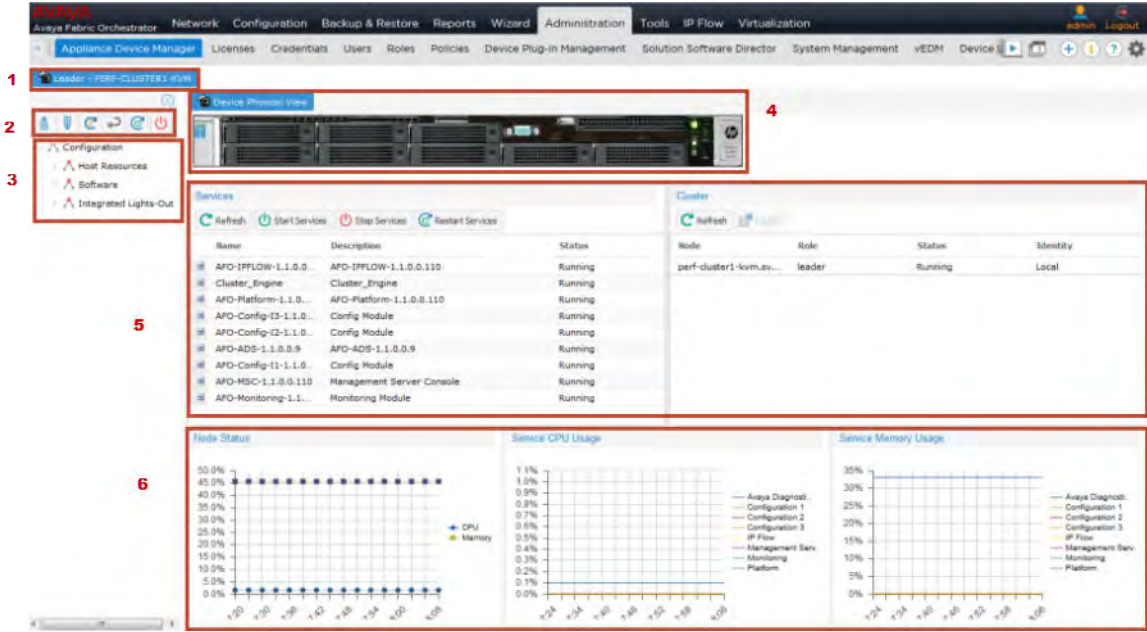
Figure 1: ADM window

1	Leader (primary server)
2	Toolbar
3	Navigation Pane
4	Device Pane
5	Grid Pane
6	Monitoring Graphs

Device Pane

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

Figure 2: Device physical view

You can use the **Rotate** icon at the top-left corner on the toolbar to rotate the view as front or back. The 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.

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.
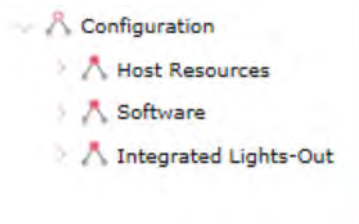
Within the **Configuration** folder, sub-folders exist. To open a sub-folder, click the arrow to the left of the folder.

To close a folder, click the arrow once.

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

Table 5: Navigation pane folders

Folder Name	Description
Configuration	Use the configuration folder to open the following sub-folders: • Host Resources • Software • Integrated Lights-Out
Host Resources	Use the Host Resources folder to gather details of the hosted services on the device.
Software	Use the software folder to gather details of the software running and installed on the device.
Integrated Lights-Out	Use the 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 details the toolbar buttons that appear in the top left navigation panel:

Table 6: Toolbar icons - navigation pane

Icon	Name	Description
	Collapse All	Use this button to collapse the sub trees in the configuration tree.
	Expand All	Use this button to expand the sub trees in the configuration tree.
	Refresh Status	Use this button to refresh all data on the grid pane screen.
	Rotate	Rotates the device view front and back.
	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.
	Appliance Reset	Use this button to restart a selected module. Click **Yes** in the confirmation window to restart a module.

The following list details some of the common buttons that appear on ADM:
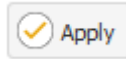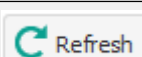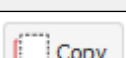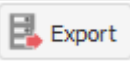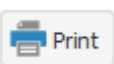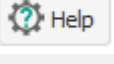
Icon	Name	Description
	Apply	The current release does not support the Apply icon.
	Refresh	Use this button to refresh all data on the grid pane screen.
	Copy	Copy data from one or more fields. ✳ **Note:** You can only copy and paste data in editable fields. The fields must have matching data type constraints.
	Paste	The current release does not support the Paste icon.
	Undo	Undo the last action.

Table continues…

Icon	Name	Description
Export	Export	Exports device information displayed in Device pane grid in to a text file.
Print	Print	Prints the device information.
Help	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 and the associated properties of the services. Use the Grid Pane to view services on the appliance.
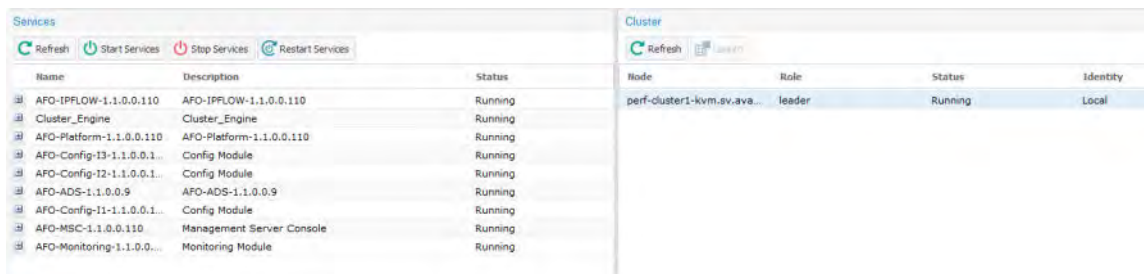
Figure 3: Grid pane

The Services section provides information about the status of the services. A status of running shows that the service is running. A status of shutoff shows that the service is not running. Click **Refresh** to update the services information.

You can start, stop, and restart services from the Services section.

The following table displays information about the services section.

Table 7: Services information

Field	Description
Name	Specifies the services that are configured on the system.
Description	Specifies a description of the service.
Status	Specifies the status. If the service status displays as running the service is running properly. If the service is not running, the status displays as shutoff.

The Cluster section provides information on the leader (primary server) and master (secondary server). You can launch information about the master (secondary server), by clicking **Launch**, and the system opens a second tab on the user interface with the master (secondary server) information.

Click on the new master (secondary server) tab to display information about the master (secondary server). Click **Refresh** to update the information in the cluster section.

Field	Description
Node	Specifies the node information
Role	Specifies the role of the node. The leader is the primary server. The master is the secondary server.
Status	Specifies the status of the node. If the node status displays as running the node is running properly. If the node is not running, the status displays as shutoff.
Identity	Specifies the identity as either local or remote.

Monitoring Graphs

Located below the Grid pane, the Monitoring Graphs display the statistical view of the CPU usage and memory usage of the services on the device. The following table describes the graphs that appear at the bottom of the ADM window.

Table 8: Monitoring Graphs

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

ADM interface configuration

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

Connecting to ADM when system is up

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

Before you begin

ADM is primarily a monitoring and configuration web-based graphical user interface (GUI) application. ADM runs on your appliance and co-resides within the KVM. ADM manages the

appliance and the services present in the appliance. You can access ADM using one of the following supported Web browsers:

- Mozilla FireFox, versions 47 and later
- Microsoft Internet Explorer, version 11
- Safari (macOS v10.8 Mountain Lion, and later)
- Ensure that the system is running.
- Note the IP address of the system.

About this task

The default username is admin and the default password is admin123. After the initial login, the administrator must update the password, and from that point onward the admin user uses the new password for the admin user.

Procedure

1. Enter the FQDN of the Platform virtual machine (VM). In the address bar, enter the IP address of the system using the following formats: `https://<FQDN of the Platform VM>` (default) or `http://<IP_address of the Platform VM>`.

   ❗ 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 the system using the Single Sign On (SSO):

   a. In the **User ID** field, type the user name.

   b. In the **Password** field, type the password.

   c. Click **Log On**.

3. On the menu bar, select **Administration** > **Appliance Device Manager**.

   The system displays the Appliance Device Manager page.

Connecting to ADM when system is down

Use this procedure to connect to ADM when the system is down.

Before you begin

ADM is primarily a monitoring and configuration web-based graphical user interface (GUI) application. ADM runs on your appliance and co-resides within the KVM. ADM manages the appliance and the services (virtual machines) present in the appliance. You can access ADM using a supported Web browser:

- Ensure that the system is down.

Procedure

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

   > **❗ 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 KVM using your login credentials:

   a. Enter `root` as the user name.

   b. Enter `Avaya_123` as the password. (default password).

3. On the menu bar, select **Administration** > **Appliance Device Manager**.

   The system displays the Appliance Device Manager page.

Host Resources

Viewing the host resources device information

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

Procedure

1. Select **Administration** > **Appliance Device Manager**.

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

3. Click **Device** to view the device information.

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.

Viewing the host resources partition information

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

Procedure

1. Select **Administration** > **Appliance Device Manager**.

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.

4. To refresh the information, click **Refresh**.

5. To copy a field, place your mouse in a field, and click **Copy**.

   The first time you copy information, you need to click **Allow access** when prompted.

6. To export information in the table into a new window, click **Export**.

7. To print information, click **Print**.

   a. Select a printer.

   b. Click **Print** again.

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.
ID	Specifies a descriptor that 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 gigabytes (GB).

Viewing the host resources file system

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

Procedure

1. Select **Administration** > **Appliance Device Manager**.

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.

4. To refresh the information, click **Refresh**.

5. To copy a field, place your mouse in a field, and click **Copy**.

   The first time you copy information, you need to click **Allow access** when prompted.

6. To export information in the table into a new window, click **Export**.

File system tab field descriptions

Use the data in the following table to use the **File System** 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 determine the operations that you can perform on the device.
Bootable	Specifies if the file system contains special files required to boot into a 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).
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.

Viewing host resources system information

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

Procedure

1. Select **Administration** > **Appliance Device Manager**.

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.

4. To refresh the information, click **Refresh**.

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.

Table continues…

Name	Description
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 user 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.

Software

Viewing the software execution information

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

Procedure

1. Select **Administration** > **Appliance Device Manager**.

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

3. Click **Software**.

   The SoftwareRunning and SoftwareInstalled sub-tabs display on the right side of the ADM window.

4. Click the **SoftwareRunning** tab.

5. To refresh the information, click **Refresh**.

6. To copy a field, place your mouse in a field, and click **Copy**.

   The first time you copy information, you need to click **Allow access** when prompted.

7. To export information in the table into a new window, click **Export**.

8. To print information, click **Print**.

   a. Select a printer.

   b. Click **Print** again.

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.
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.

Viewing the software installed information

Use this procedure to view the software installed information.

Procedure

1. Select **Administration** > **Appliance Device Manager**.

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

3. Click **Software**.

   The SoftwareRunning and SoftwareInstalled sub-tabs display on the right side of the ADM window.

4. Click the **SoftwareInstalled** tab.

5. To refresh the information, click **Refresh**.

6. To copy a field, place your mouse in a field, and click **Copy**.

   The first time you copy information, you need to click **Allow access** when prompted.

7. To export information in the table into a new window, click **Export**.

8. To print information, click **Print**.

   a. Select a printer.

   b. Click **Print** again.

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.

Table continues…

Name	Description
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.

Integrated Lights-Out

Launch iLO

Use this procedure to launch iLO.

Procedure

1. Select **Administration** > **Appliance Device Manager**.

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.

4. Enter the local username and password to login.

Viewing the iLO overview information

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

Procedure

1. Select **Administration** > **Appliance Device Manager**.

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

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

4. To refresh the information, click **Refresh**.

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.

Table continues…

Administration using Avaya Fabric Orchestrator

Name	Description
	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.
	If the OS cannot determine a unique ID, the OS 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.

Viewing the iLO system information

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

Procedure

1. Select **Administration** > **Appliance Device Manager**.

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

3. Click the **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.
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.

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.

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.

Table continues…

Name	Description
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`.
Thresholds	Specifies the type of temperature sensor.
Status	Specifies the temperature sensor condition.

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 cannot 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.

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.

Table continues…

Name	Description
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.

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 display name of the device containing the firmware.
Version	Specifies the version of the device firmware.

Viewing the iLO network information

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

Procedure

1. Select **Administration** > **Appliance Device Manager**.

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

3. Click **Network Information** to view the network information.

4. To refresh the information, click **Refresh**.

5. To export information in the table into a new window, click **Export**.

6. To print information, click **Print**.

   a. Select a printer.

   b. Click **Print** again.

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.

Table continues…

Name	Description
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`.

Viewing the iLO management log information

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

Procedure

1. Select **Administration** > **Appliance Device Manager**.

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

3. Click the **Logs** tab to view the log information.

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

4. Click **Integrated Management Log**.

5. To refresh the information, click **Refresh**.

6. To export information in the table into a new window, click **Export**.

7. To print information, click **Print**.

   a. Select a printer.

   b. Click **Print** again.

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.

Table continues…

Name	Description
Class	Specifies the iLO event log entry class designation.
LogEntryCode	Specifies the event log entry code designation as defined in the 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.

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.

Viewing the iLO thermal information

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

Procedure

1. Select **Administration** > **Appliance Device Manager**.
2. On the ADM window, select **Configuration** > **Integrated Lights-Out** from the left navigation pane.
3. Click the **Thermal** tab to view the thermal information.
4. To refresh the information, click **Refresh**.
5. To export information in the table into a new window, click **Export**.
6. To print information, click **Print**.
   a. Select a printer.
   b. Click **Print** again.

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 is `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.

Viewing the iLO physical drive information

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

Procedure

1. Select **Administration** > **Appliance Device Manager**.

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

3. Click the **Physical Drive** tab to view the CPU information.

Physical Drive 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 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 physical drive.
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.

Table continues…

Name	Description
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`.

Administration using Avaya Fabric Orchestrator

Chapter 12: Software upgrades and patching

Upgrade fundamentals

Overview

Upgrading is the process of updating the existing managed elements software version with a new version. The managed elements include the virtual machine, applications for all the elements, and devices that are managed by the system.

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 managed elements and recommends the required upgrades and updates based on your entitlements.

Solution Software Director

You can perform software upgrade and patching using the Solution Software Director. On the user interface, click **Administration** > **Solution Software Director**.

The Solution Software Director runs on the Management Server Console (MSC) virtual machine of the platform and is only accessible for authorized users.

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

You can upgrade the system using one of the following methods depending on the scenarios defined in the table below:

- Easy mode upgrade

- Advanced mode upgrade

If an upgrade is required for the MSC, the Solution Software Director completes the upgrade for the MSC first before moving on to upgrade the other components.

The following table lists different scenarios and type of upgrades.

Table 9: Type of upgrades

Scenario	Type of 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

Solution Software Director Icons

You can perform a software upgrade and patching using Solution Software Director.

Select **Administration** > **Solution Software Director** to perform a software upgrade. The system displays the home page with the following sections:

Table 10: Solution Software Director home page web interface description

Solution Software Director icon	Solution Software Director home page element	Description
	Home	Use the home page to perform software upgrade and patching. Click **Home** from the top toolbar to open the home page.
	MSC Preferences	Helps to add and define MSC settings and other properties of the system across multiple sessions. ➕ **Tip:** You can also launch **MSC Preferences** from the quick access toolbar. Click the **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 appliance in reverse chronological order. Information of the last upgrade is shown on the top.

Solution Software Director home page element	Description
System information	
License	Displays the current License type of the system.
System Status	
Application Status	Displays if the application status is `Online` or `Offline`, based on the availability of PLDS access, from the server.
Activity Logs	
Activity Logs	The Activity Logs section exists at the bottom of the Solution Software Director pages and this section is common across all the pages. Log message of the current upgrade activities are visible to all users logged on to the Solution Software Director.

Solution Software Director Home page

The following table describes the Solution Software Director Home page.

Section	Description

System Information	The system information section displays the following information:
	
	• Current Release—Displays the current system release.
	
	• Upgrade Release—Displays as none if no upgrade is underway. If an upgrade is underway, the upgrade version appears here.
	
	• License—Displays the state of the license, as one of the following:
	
	  - TRIAL—Displays if the system is running with the trial license.
	
	  - GRACE — Displays if the system is running after the trial license expired.
	
	  - ENTERPRISE — Displays if the system is running with a license acquired from PLDS.

System Status	Displays the Product Licensing and Delivery System (PLDS) connectivity that is available on the appliance. PLDS provides the ability to automatically download updates for your system. The system must have internet connectivity, and you must configure PLDS preferences by going to MSC preferences, under the preference icon. If the system is being upgraded, a message appears in this section that reads: `System upgrade in progress.`
Perform Upgrade in Easy Mode Perform Upgrade in Advanced Mode	Use the Perform Upgrade link to upgrade the system. The wizard brings you through the stages of analysis of the current system, and the compatibility and availability of new updates.
Activity Logs	As you move through the wizard and perform upgrades the activity displays in this panel and shows at what stage the upgrade is. Errors display in red and information logs display as blue.

Inventory

When you select **Perform Upgrade in Advanced Mode**, the Inventory page opens and displays the current list of each service that runs on the system.

The system displays the **Upload Matrix** or **Analysis** button dependent on the PLDS connectivity to the server. If the Solution Software Director is in online mode, the compatibility matrix downloads automatically. If the Solution Software Director is in offline mode and you have not yet uploaded the compatibility matrix, you must click **Upload Matrix**.

➕ **Tip:**

Alternatively, the compatibility matrix is also available on the Avaya support site at https://support.avaya.com/.

Solution Software Director buttons

Activity Logs

The **Activity Logs** section exists at the bottom of all the Solution Software Director pages and this section is common across all the pages of the Solution Software Director. Log messages of the current upgrade activities are visible to all users logged on to Solution Software Director.

The **Activity Logs** section 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

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 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).

Table continues…

Color Code	Description
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 the server (offline).
- Download Bundle—Displays when PLDS is accessible from the server (online).

Precheck

The **Precheck** page displays the results on a per service basis as `Pass` or `Fail` along with the description. You can perform the precheck of the downloaded or uploaded bundles by clicking on the precheck button.

If any service prechecks fail, the system blocks the upgrade. You must review the **Activity Logs** section to rectify the problem before you perform the upgrade again.

The **Activity Logs** section provides runtime updates of the upgrade activities to all users logged into Avaya Software Director.

Upgrade

The **Upgrade** page displays the download ID, filename, a short description, and progress of the upgrade. The progress column displays a green color bar when the system completes the upgrade. The upgrade is enabled only after the successful completion of the prechecks. If any services prechecks fail on the precheck page, the system blocks the upgrade.

The Upgrade page appears after the system has completed the analysis, you have uploaded needed bundles, and the system has completed the prechecks.

Solution software upgrade procedures

Accessing MSC preferences

Use MSC preferences to configure preferences related to the Management Server Console, Product Licensing and Delivery System (PLDS), and Software Library. This section provides information about launching and configuring Management Server Console (MSC) preferences.

After you configure PLDS settings, the system downloads upgrades and software bundles for future installation.

Procedure

1. To access MSC Preferences, do the following:

   a. Click the **Preferences** icon on the quick access toolbar on the top right.

   b. On the Preferences page, click **MSC** on the left navigation pane to open the MSC preferences page.

   OR

2. To access MSC Preferences from the Solution Software Director page, do the following:

   a. On the menu bar, select **Administration** > **Solution Software Director**.

   b. On the Solution Software Director page, click the **MSC Preferences** icon from the top left toolbar to open the MSC preferences page.

Upgrading using Easy mode upgrade

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

🛈 **Important:**

This release of AFO supports both HA and non-HA deployments. The system automatically detects the type of deployment and upgrade both nodes in an HA environment or upgrade a single node in a non-HA environment.

⊛ **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 using the administrator credentials.

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

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

4. Accept the end user license agreement certificate.

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 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 system and is only accessible for authorized users.

🛈 **Important:**

This release of AFO supports both HA and non-HA deployments. The system automatically detects the type of deployment and upgrade both nodes in an HA environment or upgrade a single node in a non-HA environment.

- You can perform the Advanced mode upgrade using the platform service by logging in using administrator credentials.

- On the menu bar, click **Administrator** > **Solution Software director**.

Upgrading using Advanced mode upgrade when PLDS connectivity status is online

About this task

Use this procedure 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 as an administrator.

About this task

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.

Activity Logs provide runtime updates of the upgrade activities to all logged in users of the Solution Software Director.

The system displays the **Upload Matrix** or **Analysis** button dependent on the PLDS connectivity to the server. If PLDS is in online mode the compatibility matrix downloads automatically. If PLDS is in offline mode and you have not yet uploaded the compatibility matrix, you must click **Upload Matrix** to gain access to PLDS. The compatibility matrix is available on the PLDS or on the Avaya support site at https://support.avaya.com/.

Procedure

1. Select **Administration** > **Solution Software Director.**

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

3. On the Inventory page, click **Analysis** to analyze and retrieve the latest available releases that can be upgraded.

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

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

5. Click **Download Bundle**. The system automatically downloads the bundles required for the upgrade from the PLDS.

6. Click **Start Upload**.

7. 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.

8. 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.

Color codes

The following table provides a description of the color codes.

Table 12: Color code significance

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

Upgrading using advanced mode upgrade when PLDS connectivity status is offline

About this task

Use this procedure when the PLDS connectivity status is offline and PLDS is not accessible from the server.

Before you begin

- Ensure that you are logged on as an administrator.

  > 🛈 **Important:**
  >
  > Based on the availability of PLDS access from the server, the PLDS connectivity status shows as online or offline.

About this task

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

After you attempt an upload, if a failure error message displays, see **Activity Logs** to rectify the problem and perform the upgrade. Activity Logs provide runtime updates of the upgrade activities to all logged in users of the Solution Software Director.

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.

The system displays the **Upload Matrix** or **Analysis** button dependent on the PLDS connectivity to the server. If PLDS is in online mode the compatibility matrix downloads automatically. If PLDS is in offline mode and you have not yet uploaded the compatibility matrix, you must click **Upload Matrix**. The compatibility matrix is available on the PLDS and on the Avaya support site at https://support.avaya.com/.

Procedure

1. Select **Administration** > **Solution Software Director**.

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

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

   The system displays the End User License Agreement window.

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

5. Browse to the Compatibility matrix file, and click **Open**.

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

7. 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.

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

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

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

   Choose from the following 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**.
If the requisite bundles are not available in the Software Library	Click **Browse** to upload the bundle and click **Start Upload**.

10. 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.

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

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. The system displays **Upload Compatibility Matrix** page only when PLDS is offline.

> ✴ **Note:**
>
> If the latest compatibility matrix is unavailable on the system, download the latest compatibility matrix in the software library from the PLDS or Avaya support site. For more information, see *Avaya Fabric Orchestrator Release Notes*.

Procedure

1. Select **Administration** > **Solution Software Director**.

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

3. On the Inventory page, click **Upload Matrix**.

4. Accept the End User License Agreement, and click **OK**.

5. Browse to the Compatibility Matrix file, and click **Open**.

6. Click **Upload**.

   The system displays a `success` or a `failure` message for the file uploaded.

7. Click [Analysis](#) if the file is successfully uploaded.

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

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. The system also automatically downloads the latest compatibility matrix from the Avaya support site. The **Software Library** page serves as a repository to store these bundles and compatibility matrix XML files.

2. Click Precheck on page 125 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. **Administration** > **Solution Software Director**

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

3. If the requisite bundles are not available in the **Software Library**, click **Upload Bundle**.

4. Click **Browse** to select the bundle and click **Start Upload**.

5. 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**.

6. Click Precheck on page 125 to perform the prerequisite check of the uploaded bundles.

Clearing activity logs

Use the following procedure to clear activity logs on the Solution Software Director.

Before you begin

Ensure that you are logged on as an administrator.

Procedure

1. Select **Administration** > **Solution Software Director**.

2. Click **Clear activity logs** icon on the left of the Activity Logs pane.

Saving activity logs

Use the following procedure to save activity logs on the Solution Software Director.

Before you begin

Ensure that you are logged on as an administrator.

Procedure

1. Select **Administration** > **Solution Software Director**.
2. Click **Save activity logs** icon on the left of the Activity Logs pane.
3. Choose to open or save the activity_logs.log file.
4. If you save or save as, browse to where you want to save the activity logs to your PC, then click **Save**.

Adding a file to the software library

Use the following procedure to add a file to the software library.

Before you begin

Ensure that you are logged on as an administrator.

Procedure

1. Select **Administration** > **Solution Software Director**.
2. Click the **Software library** icon on the top left menu.
3. Click **Add File** on the top left of the window.
4. Enter the download ID in the **Download ID** field.
5. Click the **Browse** icon, and browse to where the file exists.
6. Click **Open**.
7. Click **Add**.

Solution Software Director Software Library field descriptions

Use the information in the following table to understand the Software Library table.

Name	Description
Download ID	Specifies the download ID for the software.
File Name	Specifies the file name for the software.

Table continues…

Name	Description
File Size	Specifies the file size for the software.
Updated Date	Specifies the updated date for the software.
Description	Specifies the description for the software.

Refreshing the file list in the software library

Use the following procedure to refresh files in the software library.

Before you begin

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

Procedure

1. Select **Administration** > **Solution Software Director**.

2. Click the **Software library** icon on the top left menu.

3. Click **Refresh** on the top left of the window.

Deleting a file from the software library

Use the following procedure to delete a file from the software library.

Before you begin

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

Procedure

1. Select **Administration** > **Solution Software Director**.

2. Click the **Software library** icon on the top left menu.

3. Select the file you want to delete.

4. Click **Delete File**.

Viewing the software inventory online

Use the following procedure to view the software inventory while the system is online.

Before you begin

Ensure that you are logged on as an administrator.

Procedure

1. Select **Administration** > **Solution Software Director**.

2. Click the **Software library** icon on the top left menu.

Solution Software Director Inventory field descriptions

Use the information in the following table to understand the Solution Software Director Inventory table.

Name	Description
Name	Specifies the name of the system and the components included in the system.
IP Address	Specifies the IP address of the system.
Type	Specifies the type of virtual machine (VM) or component.
Current Release	Specifies the current release.

Viewing the software inventory offline

Use this procedure to view the software inventory offline.

Before you begin

Ensure that you are logged on as an administrator.

Procedure

1. Select **Administration** > **Solution Software Director**.

2. Click the **Perform Upgrade in Advanced Mode** link.

   The Inventory page displays the software inventory.

Viewing Solution Software Director upgrade history

Use the following procedure to view the Solution Software Director upgrade history.

Before you begin

Ensure that you are logged on as an administrator.

Procedure

1. Select **Administration** > **Solution Software Director**.

2. Click the **Upgrade History** icon on the top left menu.

Solution Software Director upgrade history

Use the data in the following table to understand the Solution Software Director upgrade history information.

Name	Description
Version	Specifies the software version.
Upgraded on	Specifies when the upgrade took place.

Chapter 13: Logging and Log Harvesting

Understanding Logging

A Common Logging Format (CLF) for Audit, Operation, and Security Log messages of applications is available.

Overview

Logging is a set of serviceability feature. The 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:

Table 13: 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 the system.
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 the system.

Avaya Common Logging Format (CLF)

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

The system 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.

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 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

The system provides an *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.

For more information on configuring the preferences settings related to the Logging, and Log Harvesting tasks, see Managing Preferences on page 54.

One-click log collection

You can run a single command to collect all application logs (debug/trace/operational/audit/security) into a single archive, for all issues related to troubleshooting. The command collects TFP logs on configuration, domain level information on monitoring, and system information. All logs are archived at a services level, and then at the cluster level.

Use the information in the current section to perform one-click log collection for application logs generated on the centralized server on demand in a single click.

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 is executed remotely from the Management Server Console (MSC) on every applicable system and collects the archive to a central place.

One-click log collection configuration

About this task

Use the following procedure to create a log archive of the entire appliance that contains logs of all of its services. The information includes:

- Application specific logs
- Jboss logs
- Avaya CLF logs (operational, audit, and security) files

Logs are hierarchically archived at a service level, and also at an appliance level.

The current procedure collects logs into a single archive from all the applications deployed on the system.

Procedure

1. Use SSH to login to the MSC as an admin user.

2. Run the `su − root` command on the Command Line Interface (CLI) to switch to the root user.

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

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

4. 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.

   The ZIP file contains the logs from all of the modules, including Monitoring, Configuration, Flow, MSC, and Platform logs.

Chapter 14: Licensing

System licensing

Licensing the system 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 on page 18.

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 `cluster-hostid` command. For more information, see Command Line Interface on page 17.

Procedure

1. Log on to the system.

2. On the 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 as an administrator.

Procedure

1. On the 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 as an administrator.

Procedure

1. On the 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 system.
- Install the license file on the WebLM server for the licensed product.

the

Procedure

1. On the 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 the system.

Procedure

1. On the 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 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.

Device licensing

Device licensing allows you to discover the device licenses in the network.

Viewing device licenses

About this task

Use this procedure to view the license for a device in the network.

Procedure

1. Select **Administration** > **Device Licensing**.

   A list of the devices displays.

2. If required, use the search functionality at the top of any one of the columns to search for the device.

3. When you find the device, select the + next to a device IP to view the details of the license file.

Field descriptions

Use the data in the following table to understand the Device Licensing page.

Field	Description
Device IP	The IP address for the device. Select the + to view the details of the discovered license: • License file name • License type • Generation time • Expiration time
Device MAC	The MAC address for the device.
Device Type	The type of device.
AFO Managed	Indicates whether or not the device is managed by the system.
Last Discovered	Indicates the date and time that the system last discovered the device license.

Discovering licenses

About this task

Use this procedure to discover device licenses for selected devices in the network.

Procedure

1. Select **Administration** > **Device Licensing**.

   A list of the devices displays.

2. If required, use the search functionality at the top of any one of the columns to search for a device.

3. Select the check box next to the device IP to select one or several devices. You can also select the check box at the top of the list of device IPs to select all of the devices.

4. Click **Discover Licenses**.

   When the system completes the license discovery for the selected devices, a status prompt displays.

5. Click **OK**.

   The Device Licensing page reloads and displays the updated device licenses.

Chapter 15: NBI access control

Overview

NBI Access Control simplifies which user can perform which function, by allowing the administrator to create new oAuth clients, users/credentials, specify the roles and give permissions to the endpoints/API methods that are allowed for the given role. Only the user with the AFO system administrator role can access the NBI Access Control page. Login to the AFO GUI using the system administrator credentials and navigate to **Administration** > **NBI Access Control**.

Viewing the registered clients list

About this task

Use this procedure to view the list of registered clients.

Procedure

1. Select **Administration** > **NBI Access Control**.

   The registered clients list displays.

2. To change the number of records that appear in the list, select a new value from the **Show Records** field.

3. To search for a client, enter the client name or client ID in the **Search Client** field.

Registered clients list field descriptions

Use the data in the following table to understand the Registered Client List page.

Field	Description
Client Name	Name of the client.
Client Id	Id generated for the client.
Secret Key	Value required for the authorization.
Description	Description about the client.

Table continues…

Field	Description
Token Expiry	Time in second for the token expiry
Actions	Select **Edit** to edit the registered client.
	Select **Delete** to remove the client from the list.

Registering a client

About this task

Use this procedure to register a client.

Procedure

1. Select **Administration** > **NBI Access Control**.

   The registered clients list displays.

2. On the Registered Clients List page, click **REGISTER CLIENT**.

3. On the Register client page, enter the client details.

4. Click Submit.

Registering a client field descriptions

Use the data in the following table to understand Registering a client page.

Field	Description
Client Name	Specify the name of the client.
Description	Description about the client.
Grant Type	Select the Client Credential and Resource owner password credential grant type.
	The Client Credential and Resource owner password credential are selected as the default options.
Token Expiry	Enter token expiry in seconds. (maximum 5 digits.)

Editing a client

About this task

Use this procedure to edit a client in the registered client list.

Procedure

1. Select **Administration** > **NBI Access Control**.

   The registered clients list displays.

2. Click the **Edit** icon.

3. Make the required changes.

4. Click the **Save** icon to save the changes.

Deleting a client

About this task

Use this procedure to delete a client from the registered client list.

Procedure

1. Select **Administration** > **NBI Access Control**.

   The registered clients list displays.

2. Click the **Delete** icon.

3. At the prompt to delete the client, click **Delete**.

Viewing roles

About this task

Use this procedure to view the roles.

Procedure

1. Select **Administration** > **NBI Access Control**.

2. Select **Roles** from the left navigation pane to view the assigned roles.

Viewing roles field descriptions

Use the data in the following table to understand the Roles page.

Field	Description
Name	Name of the assigned role.
Description	Description of the assigned role.

Table continues…

Field	Description
Permissions	Opens the Edit Role dialog where you can add or remove endpoint permissions.

Adding a role

About this task

Use this procedure to add a role and assign endpoint permissions.

Procedure

1. Select **Administration** > **NBI Access Control**.

2. Select **Roles** from the left navigation pane.

3. To add a role, click **Add a Role**.

4. On the Add Role page, enter a name for the role.

5. Enter a description for the role.

6. Assign endpoints to the role. In the Endpoint Permissions section, click **Add a new permission**.

7. Select the endpoint and a method.

8. Click **Save**.

Adding roles field descriptions

Use the data in the following table to understand Adding role page.

Field	Description
Role Name	Enter the role name.
Role Description	Enter the role description.
Endpoint	Assign endpoints to the role. Select the GET permission to the role. ✳ **Note:** POST, PUT, and DEL are non editable permissions.

Deleting a role

About this task

Use this procedure to delete a role.

Procedure

1. Select **Administration** > **NBI Access Control**.

2. Select **Roles** from the left navigation pane.

3. Select the role that you want to delete and click **Delete a role**.

4. At the prompt to remove the role, click **Yes**.

Viewing users

About this task

Use this procedure to view the users.

Procedure

1. Select **Administration** > **NBI Access Control**.

2. Select **Users** from the left navigation pane to view the users.

Viewing users field descriptions

Use the data in the following table to understand the Users page.

Field	Description
Name	Name of the user.
Role	Role of the user.
Email	Email for the user.
Description	Description of the user.

Adding a user

About this task

Use this procedure to add a user.

Procedure

1. Select **Administration** > **NBI Access Control**.

2. Select **Users** from the left navigation pane to view the users.

3. On the Users page, click **Add a User**.

4. On the Add/Edit Users page, enter the user details.

5. Click **Save**.

Adding a user field descriptions

Use the data in the following table to understand Adding a user page.

Field	Description
User Name	Specify a name for the user.
Password	Specify a password for the user.
Email	Specify the email for the user.
Description	Provide a description of the user.
Role	Specify the role of the user.

Deleting a user

About this task

Use this procedure to delete a user.

Procedure

1. Select **Administration** > **NBI Access Control**.

2. Select **Users** from the left navigation pane to view the users.

3. On the Users page, select the user that you want to delete.

4. Click **Delete a User**.

5. At the Remove User prompt, click **Yes**.

Chapter 16: Maintenance

Backup

Backup and restore fundamentals

Maintaining backup files can minimize downtime if the system information becomes corrupt.

Starting from this release backup and restore module will support:

- Backup and restore functionality for a single node as well as HA environment.
- Backup and restore of Cluster Engine VM along with the existing VMs.

    List of supported VMs for backup and restore:

    - Platform
    - Monitoring
    - Flow
    - Configuration
    - MSC
    - Cluster Engine

Backup options

You can perform a system backup manually or a scheduled backup at a specific time interval.

- **Manually**: The system does not perform automatic backups. You can manually backup the system using the command line interface (CLI).
- **Scheduled**: You can perform scheduled backups at a specified time 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 occurs every Sunday at 22:00 hours.

Recommendations

Use the information in this section to understand the considerations and recommendations before performing a manual 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 the system. For more information see, CLI Commands on page 18.

Backup and restore guidelines and limitations

The following are guidelines and limitations to use when backing up and restoring the 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 system is not allowed. The system performs the entire backup and restore of the applications at once.

- You cannot perform backup and restore if any of the virtual machines are corrupted.

- Upon execution of backup and restore operation, backup or restore flow will enable Cluster Engine maintenance mode.

  ⊛ **Note:**

  Failover won't happen till the backup/restore completes. After completion of backup or restore execution, maintenance mode will be disabled.

Flowchart: Performing a manual backup

Use the following process to perform a manual backup of the system.
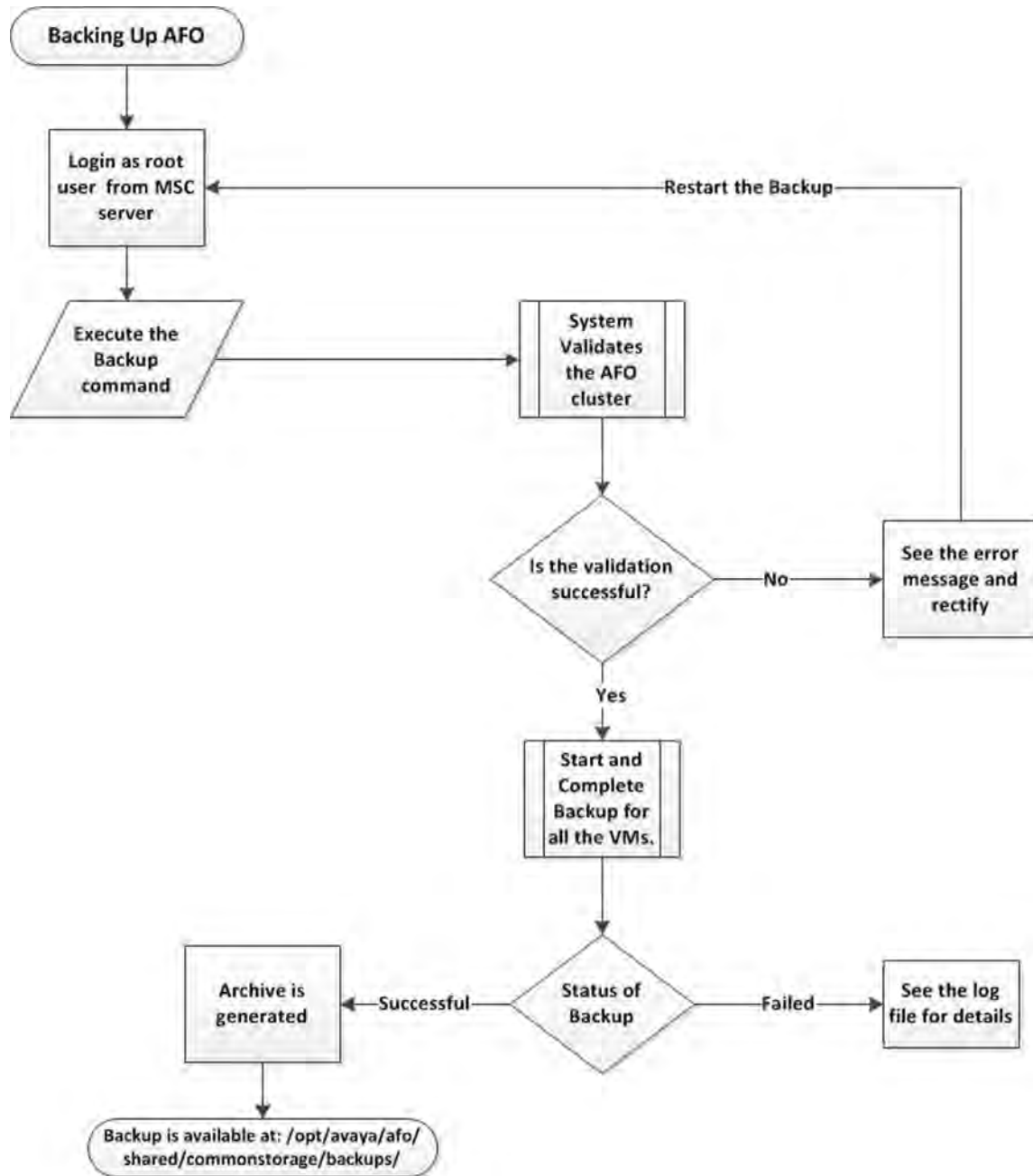
Figure 4: Flowchart: Performing a manual backup

Performing a manual backup

You can perform a manual backup at any time. Use the following procedure to perform a manual backup of the system using the command line interface (CLI).

Before you begin

- Ensure that you have SSH connectivity to the MSC VM on the primary server (leader node).
- Ensure to enable Cluster Engine maintenance mode before performing a backup.
- Ensure that you have the root username and password access credentials.

Procedure

1. Login as a root user on the MSC server.

2. Run the backup command:

   `/opt/avaya/smgr/backuprestore/backupRestoreCluster.sh --backup`

   > ⊛ **Note:**
   >
   > Make sure to enable Cluster Engine maintenance mode during the backup operation. Failover won't happen till the backup or restore completes. After completion of backup or restore execution, maintenance mode will be disabled.

   For HA systems, the system validates the cluster on the leader and master nodes for the backup procedure. If validation fails on either node the backup does not continue. The system displays the restore status for both nodes.

3. If validation is successful, continue on to the next step. Otherwise, if the validation fails, start the procedure again from the beginning.

   The system proceeds with a backup of the system when the validation is successful.

4. The system displays the status of the backup and creates an archive at `/opt/avaya/afo/shared/commonstorage/backups/` if the status is `Successful`.

   The archive does not include backup of any add-ons deployed on the cluster.

   If the system `Failed` to take backup, for more details refer to the log file located at `/opt/avaya/smgr/log/ClusterBackupRestore.log`.

Example

Backup command:

```
/opt/avaya/smgr/backuprestore/backupRestoreCluster.sh --backup
```

The system validates the cluster for the backup procedure and starts a backup of all the applications if the validation is `successful`:

```
WARNING: DO NOT use Ctrl-C to abort the script after the backup operation has started.
WARNING: During backup operation, Cluster Engine maintenance node needs to be enabled.
Failover won't happen till the backup completes. After completion of backup, maintenance
mode will be disabled. Do you wan to  proceed (y/n)?
y
Clsuter Engine maintenance node is enabled successfully.
validating the cluster for backup procedure.
Validation is successful. Proceeding with backup of cluster.

Started backup of cluster.
This procedure will take some time.

...
Completed backup of Configuration service on autodeploy-config3.avaya.com
```

Administration using Avaya Fabric Orchestrator

```
Completed backup of Configuration service on autodeploy-config2.avaya.com

Completed backup of IP Flow service on autodeploy-flow.avaya.com

Completed backup of Cluster Engine VM

Completed backup of Configuration service on autodeploy-config1.avaya.com
......
Completed backup of Monitoring service on autodeploy-monitoring.avaya.com
.................
Completed backup of Platform service on autodeploy-platform.avaya.com
...
Completed backup of Msc service on autodeploy-afo.avaya.com
------------


--------------------------------------------------------------------------
Service        Server                             Status
--------------------------------------------------------------------------
Platform       autodeploy-platform.avaya.com      Completed
Monitoring     autodeploy-monitoring.avaya.com    Completed (with warnings)
IP Flow        autodeploy-flow.avaya.com          Completed
Msc            autodeploy-afo.avaya.com           Completed
Configuration autodeploy-config1.avaya.com        Completed (with warnings)
Configuration autodeploy-config2.avaya.com        Completed (with warnings)
Configuration autodeploy-config3.avaya.com        Completed (with warnings)
ClusterEngine Cluster Engine VM                   Completed
--------------------------------------------------------------------------
Status of backup : Successful
```

The system creates an archive:

```
Creating archive...
Backup is available at: /opt/avaya/afo/shared/commonstorage/backups/
ClusterBackup_2016-10-24_19.43.zip.
This archive does not include backup of any add-ons deployed on the cluster.
```

Refer to the log file:

```
Please refer to the log file located at '/opt/avaya/smgr/log/ClusterBackupRestore.log'
for more details.
Cluster Engine maintenance node is disabled successfully.
```

Restore

Flowchart: Performing a restore

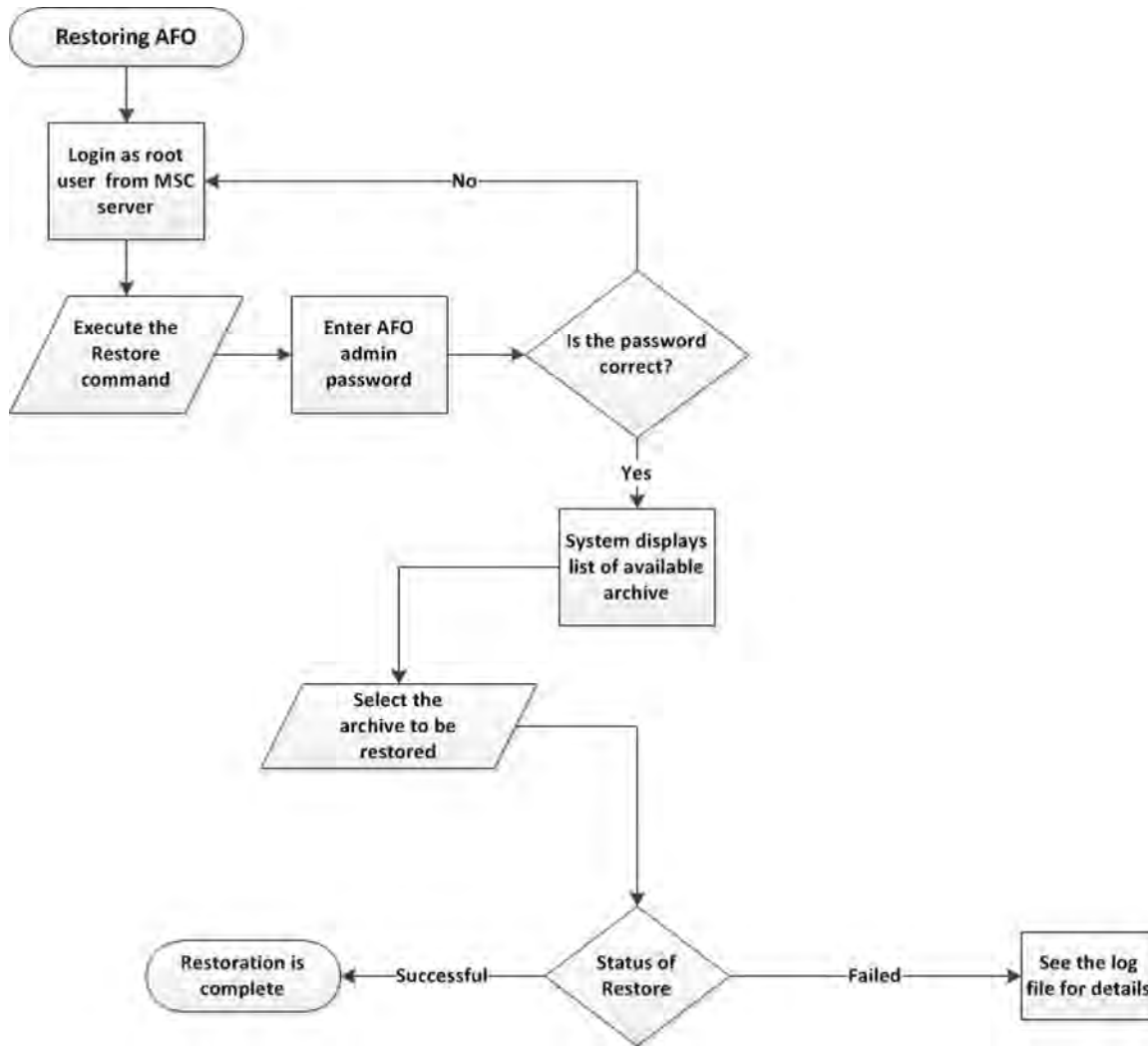You can use the following process for restoring the system.

Figure 5: Flowchart: Performing a system restore

Restoring from a backup file

You can perform a restore from a backup file at any time. Use the following procedure to restore the system from a backup using the command line interface (CLI).

Before you begin

- Ensure that you have SSH connectivity to the MSC VM on the primary server (leader node).
- Ensure that you have root username and password access credentials.
- Ensure to enable Cluster Engine maintenance mode before performing a restore.

Procedure

1. Login as root user on the MSC server.

2. Run the restore command:

```
/opt/avaya/smgr/backuprestore/backupRestoreCluster.sh --restore
```

3. Enter the AFO UI admin password.

4. Enter an archive from the list to restore.

5. The system validates the archive details.

Choice Option	Choice Description
y	Enter Y to proceed
N	Enter N to cancel the restore

6. The system automatically validates the cluster for the restore procedure and proceeds with the restore procedure after the successful completion of the validation.

The system displays the status of restore as `Successful` or `Failed`.

If the status is `Failed`, for more details refer to the log file located at `/opt/avaya/smgr/log/ClusterBackupRestore.log`.

Example

Restore command:

```
/opt/avaya/smgr/backuprestore/backupRestoreCluster.sh --restore
```

The system displays a list of the archives for restore:

```
Enter Application UI admin password: ********
The following archives are available to restore. Please choose from the list.
1. ClusterBackup_2016-11-22_13.09.zip
2. ClusterBackup_2016-11-22_13.50.zip
```

Select an archive:

```
Please choose an archive.
1
You have chosen : ClusterBackup_2016-11-22_13.09.zip. Do you want to proceed? (yes/no)
yes
************************************************************************
WARNING: You have chosen to restore the cluster. This will replace the whole data which
cannot be reverted.Do you want to proceed (y/n)?
y
************************************************************************
WARNING: During  restore operation, Cluster Engine maintenance mode needs to be enabled.
Failover won't happen till the restore completes. After completion of restore,
maintenance mode will be disabled. Do you want to proceed (y/n)?
y
Cluster Engine maintenance mode is enabled successfully.

Validating the cluster for restore procedure.
Validation is successful. Proceeding with restore of cluster.

Restore of cluster has been started. This procedure will take some time.

...
Executing restore of Platform service on AutoDEPLOY-platform.avaya.co.in
Restoration is complete for Platform service on AutoDEPLOY-platform.avaya.co.in

.Executing restore of Monitoring service on AutoDEPLOY-monitoring.avaya.co.in
......
Restoration is complete for Monitoring service on AutoDEPLOY-monitoring.avaya.co.in
```

```
Executing restore of Cluster Engine VM
...
Restoration is complete for Cluster Engine VM
Executing restore of Configuration service on AutoDEPLOY-config1.avaya.co.in

Executing restore of IP Flow service on AutoDEPLOY-flow.avaya.co.in

Restoration is complete for IP Flow service on AutoDEPLOY-flow.avaya.co.in

.......................
Restoration is completed for Msc service on AutoDEPLOY-afo.avaya.co.in
...
Restoration is complete for Configuration service on AutoDEPLOY-config1.avaya.co.in

Executing restore of Configuration service on AutoDEPLOY-config2.avaya.co.in
.......................
Restoration is complete for Configuration service on AutoDEPLOY-config2.avaya.co.in

Executing restore of Configuration service on AutoDEPLOY-config3.avaya.co.in
...........................
Restoration is complete for Configuration service on AutoDEPLOY-config3.avaya.co.in


---------------------------------------------------------------------------
Service        Server                              Status
---------------------------------------------------------------------------
Platform       AutoDEPLOY-platform.avaya.co.in     Completed
Monitoring     AutoDEPLOY-monitoring.avaya.co.in   Completed (with warnings)
IP Flow        AutoDEPLOY-flow.avaya.co.in         Completed
Msc            AutoDEPLOY-afo.avaya.co.in          Completed
Configuration AutoDEPLOY-config1.avaya.co.in       Completed (with warnings)
Configuration AutoDEPLOY-config2.avaya.co.in       Completed (with warnings)
Configuration AutoDEPLOY-config3.avaya.co.in       Completed (with warnings)
ClusterEngine Cluster Engine VM                    Completed
---------------------------------------------------------------------------
Status of restore : Successful
Cluster Engine maintenance mode is disabled successfully.
-----------------------------------------------------------------------------
```

```
Please refer to the log file located at '/opt/avaya/smgr/log/ClusterBackupRestore.log'
for more details.
```

Viewing an archive

Use this task to view the details of an archive.

Before you begin

Ensure that you have completed a recent backup of the system.

Procedure

Run the following command to view the details of an archive.

```
/opt/avaya/smgr/backuprestore/backupRestoreCluster.sh --view
```

Chapter 17: Resources

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.

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.

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 Network Management 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.	System administrator
Network Configuration using Avaya Fabric Orchestrator, NN48100–501	Configuring and managing Avaya Enterprise family of devices from discovered network.	System administrator
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 the system, to help the data center administrator to configure the network changes that apply to the data center.	System administrator

Table continues…

Document title	Use this document for:	Audience
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	System administration procedures.	System administrator
Avaya Network Management Traps and Trends Reference, NN48100–700	Viewing a list of supported traps and trends.	System administrator
Avaya Network Management Supported Devices, Device MIBs, and Legacy Devices Reference, NN48100–701	Confirming support for devices and MIBs.	System administrator
Troubleshooting Avaya Fabric Orchestrator, NN48100–702	Troubleshooting information for the system.	System administrator

Searching a documentation collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.

2. Navigate to the folder that contains the extracted files and open the file named *<product_name_release>*.pdx.

3. In the Search dialog box, select the option **In the index named *<product_name_release>*.pdx**.

4. Enter a search word or phrase.

5. Select any of the following to narrow your search:

   - Whole Words Only
   - Case-Sensitive
   - Include Bookmarks
   - Include Comments

6. Click **Search**.

The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

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**.
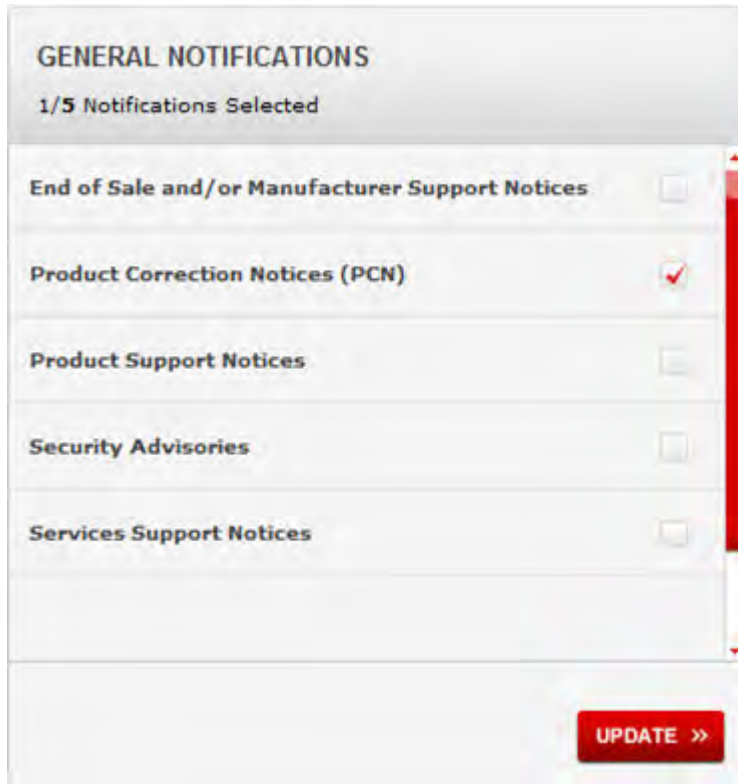
6. Click **OK**.

7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.
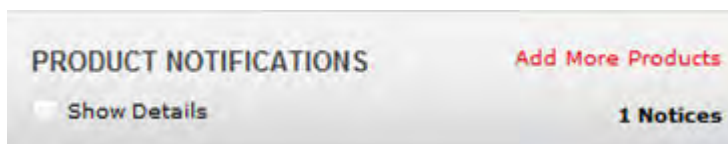
8. Scroll through the list, and then select the product name.

9. Select a release version.

10. Select the check box next to the required documentation types.

11. Click **Submit**.