



Avaya Configuration and Orchestration Manager Fundamentals

Release 3.0.1
NN47226-100
Issue 06.02
February 2013

Notice

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

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its 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 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 its hardware and Software ("Product(s)"). 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: <http://support.avaya.com>. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; 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. "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.

Licence types

Designated System(s) License (DS). End User may install and use each copy 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, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at <http://support.avaya.com/LicenseInfo> under the link "Heritage Nortel Products". 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 (in the event the applicable Documentation permits installation on non-Avaya equipment) 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, or hardware provided by Avaya. All content on this site, the documentation 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.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that 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"). 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 Documentation or on Avaya's website at: <http://support.avaya.com/Copyright>. You agree to the Third Party Terms for any such Third Party Components.

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: <http://support.avaya.com>. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya Aura® is a registered trademark of Avaya Inc.

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation 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, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <http://support.avaya.com>.

Contact Avaya Support

See the Avaya Support website: <http://support.avaya.com> for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <http://support.avaya.com>, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction	7
Purpose	7
Related resources	7
Chapter 2: New in this release	9
Features	9
Other changes	10
Chapter 3: Configuration and Orchestration Manager overview	11
Navigation pane	12
Chapter 4: Configuration and Orchestration Manager logon	15
Logging on to COM	15
Chapter 5: Network discovery	19
Topology Manager	19
IEEE 802.1ab	19
Enabling discovery with 802.1ab	21
Contents pane	22
Latest Logs pane	29
Links	30
Chapter 6: User management	31
Avaya UCM role	31
Viewing existing users	33
Adding a new local or external user	34
Variable definitions	36
Disabling a user	36
Deleting a user	37
Chapter 7: Licensing	39
License restriction	39
Node based licensing for COM	39
Adding a license	40
Exporting a license	41
Generating a licensing report	41
Refreshing the license information	42
Chapter 8: Configuration and Orchestration Manager administration	43
Access Control	43
Preferences	45
Device credentials	54
Plugins inventory	62
Audit log	67
Chapter 9: Device inventory and group management	69
Device Inventory View	69
Device Group Manager	70
Adding a device group	71
Deleting a device group	72
Adding a user group	73
Editing a user group	74

Deleting a user group.....	74
Inventory Manager.....	75
Toolbar commands.....	75
Menu bar commands.....	76
Chapter 10: Managers overview.....	79
VLAN Manager.....	79
MultiLink Trunking Manager.....	80
Security Manager.....	80
Routing Manager.....	81
Trap/Log Manager.....	81
Virtual Routing Manager.....	82
Multicast Manager.....	82
Bulk Configuration Manager.....	83
VSN Manager.....	83
Multimedia Manager.....	84
Trap Viewer.....	84
Syslog Viewer.....	85
Chapter 11: Wizards and templates overview.....	87
Wizards management.....	87
Templates management.....	89
Chapter 12: Maintenance.....	91
Starting the SmartDiff Tool.....	91
Viewing the TFTP Server.....	93
MIB Browser.....	97
Accessing the Port Scanner.....	104
Managing Scheduled Tasks.....	108
Launching CLI*manager.....	110
Launching the Configuration Auditing Tool.....	117
Chapter 13: Supported devices.....	119
Chapter 14: Appendix Recommendations and deployments.....	121
COM installation server.....	121
Rediscovery of devices.....	121
Internet browser Settings.....	122

Chapter 1: Introduction

Purpose

This document provides information and procedures for using and administering the Avaya Configuration and Orchestration Manager (COM) application. Configuration and Orchestration Manager provides you with an intuitive interface to configure, manage, and provision the Avaya enterprise family of devices, such as Avaya Ethernet Routing Switches, Avaya Ethernet Switches, Legacy BayStack switches, Business Policy Switches 2000™ operating within the same local area network, and Wireless Local Area Network (WLAN) devices. Configuration and Orchestration Manager is a management system that manages multiple network devices.

Avaya Configuration and Orchestration Manager Fundamentals (NN47226–100) is intended for administrators and users of the COM application.

Related resources

Related topics:

[Documentation](#) on page 7

[Training](#) on page 8

[Avaya Mentor videos](#) on page 8

[Support](#) on page 8

Documentation

See the following related documents:

Title	Purpose	Link
Avaya Configuration and Orchestration Manager Fundamentals (NN47226-100)	Fundamentals	http://support.avaya.com

Title	Purpose	Link
Avaya Configuration and Orchestration Manager Installation (NN47226-300)	Deployment	http://support.avaya.com
Avaya Configuration and Orchestration Manager Administration (NN47226-600)	Administration	http://support.avaya.com
Avaya Bulk Configuration Manager Fundamentals (NN48021-100)	Fundamentals	http://support.avaya.com

Training

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

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Go to <http://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 site.

Support

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

Chapter 2: New in this release

The following sections detail what's new in *Avaya Configuration and Orchestration Manager Fundamentals* (NN47226-100) for Release 3.0.1.

- [Features](#) on page 9
- [Other changes](#) on page 10

Features

See the following sections for information about feature changes:

Enhancements

Avaya Configuration and Orchestration Manager (COM) 3.0.1 introduces the following enhancements:

- Device Group Manager full support is available to all license levels including the base license.
- The Actions menu is reintroduced for the COM Inventory Manager.

Device support

Avaya Configuration and Orchestration Manager (COM) 3.0.1 supports the following devices:

- VSP 7000 v10.2 — Includes L2-SPBM capability.
- ERS 45xx v5.6.1 and v5.6.2 — Limited support for new versions; includes Discovery and EDM plug in support.
- ERS 48xx v5.6.1 and v5.6.2 — Limited support for new versions; includes Discovery and EDM plug in support.
- ERS 55xx v6.3 — Limited support for new versions; includes Discovery and EDM plug in support.
- ERS 56xx v6.3 — Limited support for new versions; includes Discovery and EDM plug in support.

Bug fixes

For more information about bugs that have been fixed for Avaya Configuration and Orchestration Manager (COM) release 3.0.1, see *Avaya Configuration and Orchestration Manager Release Notes*.

Licensing changes

You require a new license if you upgrade to Avaya Configuration and Orchestration Manager (COM) 3.0.1 from release 2.3 or 2.3.x, or 3.0 if you use a VMWare Virtual Machine. If you upgrade from 3.0 using a physical machine or a non-VMWare Virtual Machine, you do not require a new license.

Other changes

See the following sections for information about changes that are not feature-related.

Introduction chapter

The Introduction chapter replaces the Purpose of this document chapter.

Chapter 3: Configuration and Orchestration Manager overview

Avaya Configuration and Orchestration Manager (Avaya COM) provides you with an intuitive interface to configure, manage, and provision the Avaya enterprise family of devices, such as Avaya Ethernet Routing Switches, Avaya Ethernet Switches, Legacy BayStack switches, Business Policy Switches 2000™ operating within the same local area network, and Wireless Local Area Network (WLAN) devices.

Configuration and Orchestration Manager is a management system that manages multiple network devices, and provides management for services across different elements.

Configuration and Orchestration Manager is a Web-based, platform-independent application that allows you to save the error log, preferences, and communities in the application.

* Note:

To run COM, you do not require Java Runtime Environment (JRE). The JRE 1.6.0.22 is bundled with COM.

For more information about operating systems, devices, and software releases supported by Configuration and Orchestration Manager, see *Avaya Configuration and Orchestration Manager Administration* (NN47226-600).

Configuration and Orchestration Manager provides topology driven multiuser, multidevice configuration and provisioning features, and off-box element management features that includes COM and EDM management base features.

For more information about how to install Configuration and Orchestration Manager, see *Avaya Configuration and Orchestration Manager Installation* (NN47226-300).

COM features

Configuration and Orchestration Manager has the following features:

- COM 3.0.1 is a Web-based element manager and supports both Internet Explorer and Firefox browsers.
- COM is supported by dynamic HTML (DHTML). DHTML is a combination of HTML, JavaScript, and Cascading Style Sheets (CSS). To use DHTML, JavaScript and CSS must be enabled on the browser.
- COM supports wizards and templates for complex multidevice configuration management simplification.
- COM supports device configuration management.
- COM is supported across Windows, and Linux platforms.

- COM provides a consistent graphical user interface (GUI) across COM and submanagers, and provides a single point of access to the submanagers.
- COM provides access control and security using community strings, SNMPv3 USM, and SSH.

Navigation

- [Navigation pane](#) on page 12

Navigation pane

The Navigation pane is located on the left side of the Configuration and Orchestration Manager (COM) main window. By default, the Managers panel opens when you access COM.

*** Note:**

The options that appear in the Navigation pane vary depending on the user tool you select. For more information about options, see [Access Control](#) on page 43.

The Navigation pane includes the following panels for all COM features:

- **Admin**—Contains Access Control, Preferences, Device Credentials, User Management, Licensing, Plugins Inventory, and Audit Log.
- **Devices**—Contains Device Inventory View, Device Group Manager, and Inventory Manager.
- **Managers**—Contains VLAN Manager, MultiLink Trunking Manager, Security Manager, Routing Manager, Trap/Log Manager, Virtual Routing Manager, Multicast Manager, Bulk Configuration Manager, Virtual Services Network (VSN) Manager, Multimedia Manager, Trap Viewer, and Syslog Viewer.
- **Wizards**—Contains VLAN, SMLT, and VSN wizards.
- **Templates**—Contains Template Manager.
- **Tools**—Contains SmartDiff Tool, TFTP Server, MIB Browser, Port Scanner, Scheduled Tasks, CLI*manager, and Config Auditing tool.

The Navigation pane displays the contents pane. In the Navigation pane, click (+) to expand a panel, and click (-) to collapse a panel. To collapse the Navigation pane, click (<<).

The following figure shows the Configuration and Orchestration Manager Navigation pane.

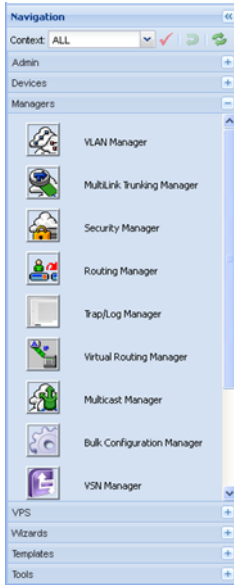


Figure 1: Configuration and Orchestration Manager Navigation pane

Chapter 4: Configuration and Orchestration Manager logon

This section describes how to start and log on to Avaya Configuration and Orchestration Manager (COM).

For more information about how to install Configuration and Orchestration Manager, see *Avaya Configuration and Orchestration Manager Installation* (NN47226-300).

Navigation

- [Logging on to COM](#) on page 15

Logging on to COM

Perform the following procedure to start the COM application.

Before you begin

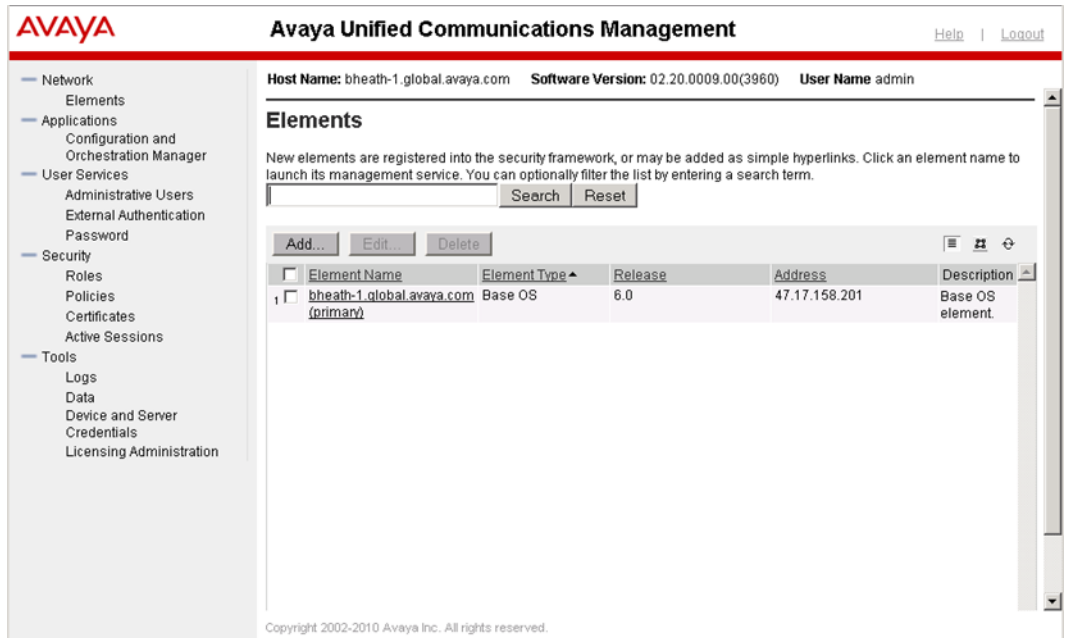
- You must install COM.
- If you are logging on with a client PC, you require Internet Explorer 7, 8 or 9, or Firefox 3.6, 9, or 10.

Procedure

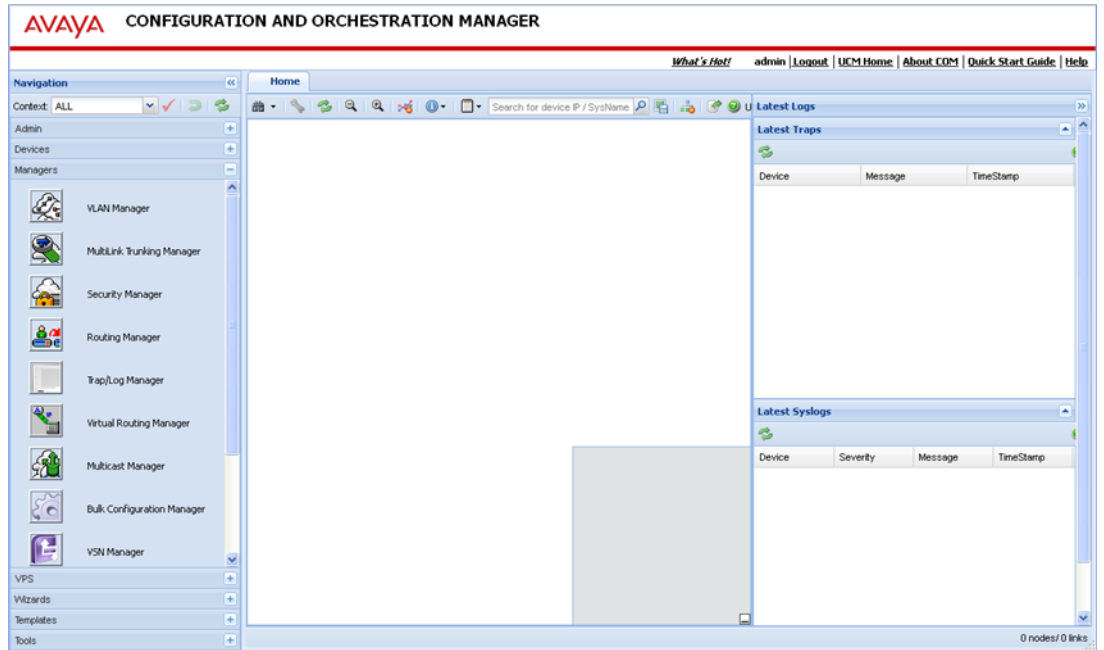
1. Start a Web browser supported by COM.
2. In the **Address** field, enter the Fully Qualified Device Name (FQDN) of the COM server.



3. In the **User ID** field, enter the installed COM user ID.
 - The default user ID is **admin**.
4. In the **Password** field, enter the installed COM password.
5. Click **Log In**.



6. In the left Navigation pane, select **Applications**, and then click **Configuration and Orchestration Manager**.



Chapter 5: Network discovery

This chapter provides an overview of the Avaya Configuration and Orchestration Manager (COM) network discovery applications, including the topology manager.

Topology Manager

The main COM window is also referred to as the Topology Manager. The Topology Manager provides a graphical view of a network of devices that support the Bay Networks Autotopology Discovery Protocol or SONMP.

IEEE 802.1ab

The Topology Manager supports the discovery of devices using IEEE 802.1ab, Station and Media Access Control Connectivity Protocol, or Link Layer Discovery Protocol (LLDP). The Topology Manager uses both 802.1ab and the Bay Networks Autotopology Discovery Protocol to discover the devices on the network.

With 802.1ab, stations connected to a LAN can advertise their capabilities to each other, enabling the discovery of physical topology information for network management. The 802.1ab-compatible stations can consist of any interconnection device including PCs, IP Phones, switches, and routers. Each station stores 802.1ab information in a standard Management Information Base (MIB), making it possible for Configuration Orchestration Manager (COM) to access the information.

With 802.1ab, COM can discover certain configuration inconsistencies or malfunctions that can result in impaired communications at higher layers, such as duplex mismatches.

Each 802.1ab station:

- advertises connectivity and management information about the local station to adjacent stations on the same 802 LAN.
- receives network management information from adjacent stations on the same LAN.

The following Avaya devices support 802.1ab:

- Ethernet Routing Switch 55xx Release 5.0
- Ethernet Routing Switch 8300 Release 3.0
- Ethernet Routing Switch 45xx Release 5.0
- Ethernet Routing Switch 25xx Release 4.0
- Ethernet Switch 325/425 Release 3.6
- Ethernet Switch 470/460 Release 3.7
- Avaya IP Phones

With 802.1ab support, COM is not restricted to the discovery of Avaya devices, and can discover any 802.1ab-enabled devices on the network, including third-party switches, routers, and IP Phones. Configuration Orchestration Manager can also display MED devices in the network.

! Important:

Configuration Orchestration Manager can only discover third-party 802.1ab-enabled devices on the network, and cannot provide management for these devices.

The following figure shows an example of how 802.1ab works in a network.

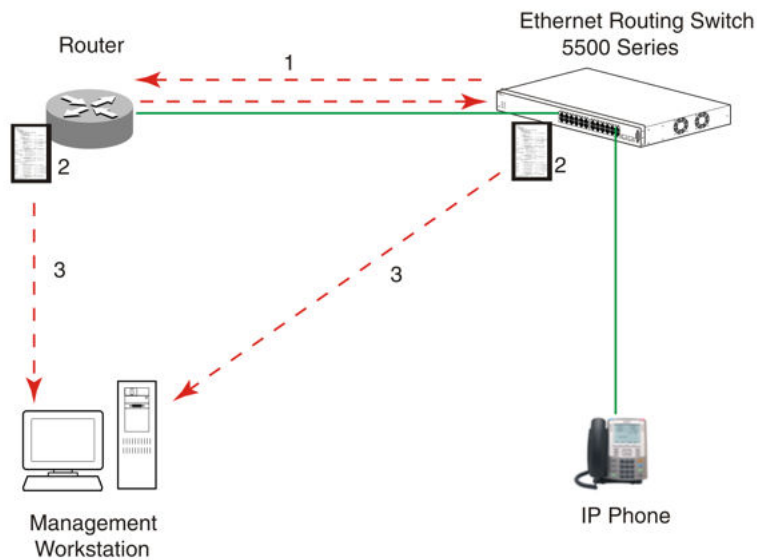


Figure 2: How 802.1ab works

1. The Ethernet Routing Switch and 802.1ab-enabled router advertise chassis/port IDs and system descriptions to each other.
2. The devices store the information about each other in local MIB databases, accessible by using SNMP.
3. A management workstation running COM retrieves the data stored by each device and builds a network topology map.

Both Avaya and third-party devices are displayed.

Enabling discovery with 802.1ab

To enable discovery of a device through 802.1ab, you must enable the following TLVs on the device:

- System Name TLV
- System Capabilities TLV
- Management Address TLV

To enable discovery of MED endpoints, you must also enable the MED TLVs on those endpoints.

For more information about configuring 802.1ab on your device, refer to the documentation for your device.

The following table describes the parts of COM main window.

Table 1: Parts of COM window

Parts	Description
Navigation pane	From the Navigation pane, you can navigate all the panels supported by COM. For more information, see Navigation pane on page 12.
Contents pane	Displays a view of all the discovered devices and their relationship. For more information, see Contents pane on page 22.
Latest Logs pane	Displays the last 15 traps and syslogs sent to COM from various devices. For more information, see Latest Logs pane on page 29.
Links	From the links available in the upper right corner of the COM main window, you can logout, access UCM home, view COM details, access the COM Quick Start Guide, and view online Help. For more information, see Links on page 30.

Contents pane

The Contents pane provides a view of all the discovered devices and their relationship on the Home tab. You can use the tool bar on the Contents pane to manage discovered devices on the topology map. You also can use the right-click menu options on the Contents pane to perform device query and administrative management.

The following sections contain information about the tool bar and right-click menu options.

Related topics:

[Toolbar options](#) on page 22

[Right-click menu options](#) on page 25

Toolbar options

You can use the tool bar buttons on the **Home** tab to manage the topology map. For example, you can zoom in and out of the device view, import or export device view values, or discover a topology.

The following table lists the tool bar options that you can use to manage your topology map.

Table 2: Home tab tool bar options

Option	Description
Discover Topology	<p>Use this option to perform the following actions:</p> <ul style="list-style-type: none"> • Discover topology from seed • Schedule a Discovery <p>You have the option to run a discovery based on a seed value. You also have the option to configure the COM application to run scheduled network discovery events. These events can occur once or repeatedly according to specific months, days of the week, date, and time.</p>
Set Discovery Preferences	<p>Before starting a discovery for the COM system, you can enter the discovery preferences such as Seed, Hop Count, and Landing Page. You also can set the COM application to run one of the following types of discoveries: new or merged.</p>
Refresh Device Topology	<p>Use this option to refresh the topology view. The COM application communicates with the server to get the latest discovered devices.</p>
Zoom Out	<p>Use this option to zoom out the topology view.</p>
Zoom In	<p>Use this option to zoom in the topology view.</p>
Clear Highlights	<p>Use this option clear the existing highlights on the topology map.</p>
View Device Information	<p>Use this option to display the port names, device types, and Link details like link speed, type, mismatch, and duplex for devices in your topology. The View Device Information button has the following options for your use:</p> <ul style="list-style-type: none"> • Display port names — Select this button to display port names on the topology map. • Toggle Addr / Name — Select this button to toggle the name and address of the device. • Link data — Select this button to perform the following actions: view link speeds, duplex, types, mismatch, and clear highlights.
Perform Device Action	<p>Use this option to perform the following actions on a topology map device:</p> <ul style="list-style-type: none"> • view port status • view connections • ping devices

Option	Description
	<ul style="list-style-type: none"> • view device properties • view a topology dump • view learned MAC addresses • launch an element manager • perform the following administrative actions: <ul style="list-style-type: none"> - create a group - update device topology - change IP address <p>You also can access these options through the right-click menu of a device on the topology map or inventory grid.</p>
Search for device IP / SysName	<p>Use this option to search and highlight an IP address you are looking for. You can search based on:</p> <ul style="list-style-type: none"> • a partial or full IP address • IPv4 format • IPv6 format <p>! Important:</p> <p>If the device is not found, then a topology dialog box appears showing, No additional matches found.</p>
Save Topology	<p>Use this option to save the current topology and export it to an XML file which you can load into COM again. This provides a way for you to save multiple topologies without having to do a rediscovery. In previous versions of COM, if you saved the layout of a topology and rediscovered the network, the previously discovered devices maintain their layout position thereby eliminating the need to relay out the topology after each discovery.</p>
Clear saved Topology	<p>Use this option to return to the topology that you had previously saved.</p>
Import/Export Topology	<p>Use this option to export in xml and csv, and import in xml formats.</p>
Reachable/Unreachable state	<p>Use this option to display the connection status of the listed devices. The devices in the topology view show an orange color to indicate the unreachable status. Unreachable status means that the device did not respond to SNMP queries from COM because the device was down or because the SNMP credentials</p>

Option	Description
	provided to COM are not correct for the device in the unreachable state.
Device navigation window	You use the device navigation window (also called the panning window) to easily pan through the whole map to focus on a specific area of the network.

Right-click menu options

You can use the right-click menu on the Home tab to manage devices on the topology map. To access the right-click menu options, right-click a device on the topology map.

One set of device actions includes query management such as ping devices, connection information, device properties, and port status. The second set of device actions includes administration management, such as update device topology and change IP address.

You also can access the right-click menu options by selecting **Device Inventory View**, and then clicking **Perform Device Action**.

The following tables describe the device management options available from the Home tab and the Device Inventory View.

- [Device management options from the right-click menu on the topology](#) on page 25
- [Device management options from the Home tab Perform Device Action button](#) on page 27
- [Device management options from the Device Inventory View Perform Device Action button](#) on page 28

The following table lists the device management options available after you right-click on a device on the topology.

Table 3: Device management options from the right-click menu on the topology

Menu option	Description
Ping...	Use this option to ping the selected device from the server.
Show Connections	Use this option to display the neighbors of a device on the topology map. It does not display live connections, only what is on the topology map.
Properties	Use this option to display the following properties of the device: <ul style="list-style-type: none"> • Name • IP address • Device type • Location

Menu option	Description
	<ul style="list-style-type: none"> • Contact • Version • Uptime • Description
Launch Element Manager	Use this option to launch the element manager for the selected device.
Show All Traps For Device	Use this option to show all traps for a device. You can select this option by right-clicking on a device only.
Show Trap Highlight Details	Use this option to show trap highlight details of a device. You can select this option by right-clicking on a device only.
Port Status	Use this option to display the status of the port. <ul style="list-style-type: none"> • green—the port is in-service • red—the port is out-of-service • blue—the port is being tested
Dump Topology	Use this option to display the topology based on the real-time queries of devices.
Learned Mac Addresses	Use this option to display the learned Mac addresses on the selected device.
Administrative Actions	Use this option to change the device attributes by performing one of the following actions: <ul style="list-style-type: none"> • Create a Group—This option appears on the topology map of the COM Home tab only. • Update device topology • Change device IP Address • Close The administrative actions prompt the system to discover a change to a single device with a one hop count. When the discovery is complete, the COM application updates the database with the discovered information.
Close	Closes the drop down menu.

The following table lists the device management options available after you select a device on the topology map, and then click on the Perform Device Action button from the Home tool bar.

Table 4: Device management options from the Home tab Perform Device Action button

Menu option	Description
Show Port Status	Use this option to display the status of the port: <ul style="list-style-type: none"> • green—the port is in-service • red—the port is out-of-service • blue—the port is being tested
Show Connections	Use this option to display the neighbors of a device on the topology map. It does not display live connections, only what is on the topology map.
Ping Device	Use this option to ping the selected device from the server.
Show Properties	Use this option to display the following properties of the device: <ul style="list-style-type: none"> • Name • IP address • Device type • Location • Contact • Version • Uptime • Description
Dump Topology	Use this option to display the topology based on the real-time queries of devices.
Learned Mac Address	Use this option to display the learned Mac addresses on the selected device.
Launch Element Manager	Use this option to launch the element manager for the selected device.
Administrative Actions	Use this option to change the device attributes by performing one of the following actions: <ul style="list-style-type: none"> • Create a Group—This option appears on the topology map of the COM Home tab only. • Update device topology • Change device IP Address The administrative actions prompt the system to discover a change to a single device with a one hop count. When the discovery finishes, the COM application updates the database with the discovered information.

The following table lists the device management options available from the Device Inventory View after you right-click on a selection on the inventory grid, or after you click the Perform Device Action button on the Device Inventory View tool bar.

Table 5: Device management options from the Device Inventory View Perform Device Action button

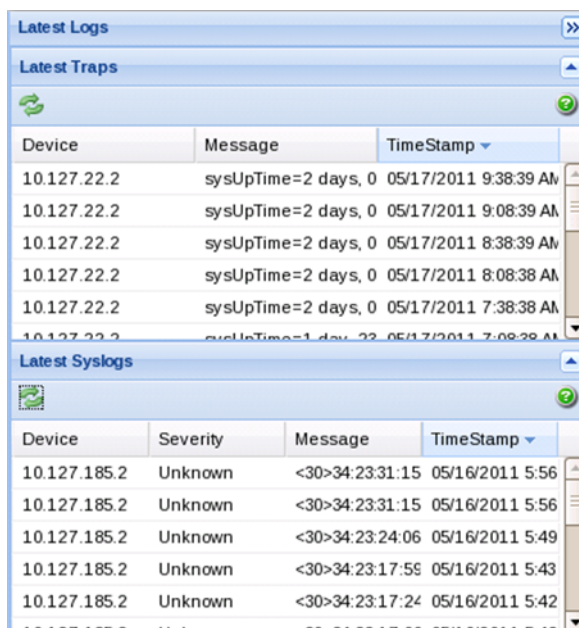
Menu option	Description
Show Port Status	Use this option to display the status of the port. <ul style="list-style-type: none"> • green—the port is in-service • red—the port is out-of-service • blue—the port is being tested
Ping Device	Use this option to ping the selected device from the server.
Show Properties	Use this option to display the following properties of the device: <ul style="list-style-type: none"> • Name • IP address • Device type • Location • Contact • Version • Uptime • Description
Dump Topology	Use this option to display the topology based on the real-time queries of devices.
Learned Mac Address	Use this option to display the learned Mac addresses on the selected device.
Launch Element Manager	Use this option to launch the element manager for the selected device.
Administrative Actions	Use this option to change the device attributes by performing one of the following actions: <ul style="list-style-type: none"> • Update Device Topology • Change IP Address The administrative actions prompt the system to discover a change to a single device with a one hop count. When the discovery is complete, the COM application updates the database with the discovered information.

Latest Logs pane

The Latest Logs pane provides a view of the latest traps and the latest syslogs, and displays the last 15 syslogs and traps sent to Configuration and Orchestration Manager (COM) from various devices. A refresh button is available in the Latest Syslogs and Latest Traps panels that always requests the last 25 logs or traps from the server. You can collapse the Latest Logs pane to maximize the topology area.

When you open a new tab, all the existing tabs, topology, latest logs, and latest traps, become inactive.

The following figure is an example of the Latest Logs pane.



The screenshot shows the 'Latest Logs' pane with two sub-panels: 'Latest Traps' and 'Latest Syslogs'. Both panels have a refresh button (circular arrow icon) and a help icon (question mark in a circle). The 'Latest Traps' table has columns for Device, Message, and TimeStamp. The 'Latest Syslogs' table has columns for Device, Severity, Message, and TimeStamp.

Device	Message	TimeStamp
10.127.22.2	sysUpTime=2 days, 0	05/17/2011 9:38:39 AM
10.127.22.2	sysUpTime=2 days, 0	05/17/2011 9:08:39 AM
10.127.22.2	sysUpTime=2 days, 0	05/17/2011 8:38:39 AM
10.127.22.2	sysUpTime=2 days, 0	05/17/2011 8:08:38 AM
10.127.22.2	sysUpTime=2 days, 0	05/17/2011 7:38:38 AM
10.127.22.2	sysUpTime=1 day, 23	05/17/2011 7:08:38 AM

Device	Severity	Message	TimeStamp
10.127.185.2	Unknown	<30>34:23:31:15	05/16/2011 5:56
10.127.185.2	Unknown	<30>34:23:31:15	05/16/2011 5:56
10.127.185.2	Unknown	<30>34:23:24:06	05/16/2011 5:49
10.127.185.2	Unknown	<30>34:23:17:59	05/16/2011 5:43
10.127.185.2	Unknown	<30>34:23:17:24	05/16/2011 5:42
10.127.185.2	Unknown	<30>34:23:17:06	05/16/2011 5:40

Figure 3: Latest logs pane

The Latest Logs pane contains the following panels.

Latest Traps

The Latest Traps panel lists the latest traps COM receives from traps sent by devices. The devices are programmed with the COM IP address so that COM can receive the device traps. The Latest Traps panel includes a refresh button to provide the most current list, the device IP address, message, and timestamp.

Latest Syslogs

The Latest Syslogs panel lists the latest syslogs for a device, and includes a refresh button. Each device syslog includes a severity level, message, and timestamp.

Links

The following links are located at the upper right corner of the Configuration and Orchestration Manager (COM) main page.

- **What's Hot!**
- **admin**—Displays the current logged in user name.
- **Logout**—Logs you off from the Avaya Unified Communications Management (UCM) and returns you to the logon page.
- **UCM Home**—Opens the UCM page.
- **About COM**—Opens a dialog box that provides information about COM, such as version, revision, and build. If you are using node-based licensing, then the number of nodes supported by the license appears in the dialog box. If you are using the FullApp license, there is no change.
- **Quick Start Guide**—Outlines the set up steps that the COM administrator requires after a new COM is installed. This link guides the administrator through various initial steps such as creating users, discovering the network, assigning device and multi-element manager permissions to the users. This link also guides you through the one time setup required on the client machine.
- **Help**—Starts the online help.

The following figure displays COM links.



Figure 4: COM Links

Chapter 6: User management

This section provides information about managing users, and creating and managing the capabilities of users by assigning roles. The administrator can perform the user management tasks required to manage users within the UCM.

Navigation

- [Avaya UCM role](#) on page 31
- [Viewing existing users](#) on page 33
- [Adding a new local or external user](#) on page 34
- [Disabling a user](#) on page 36
- [Deleting a user](#) on page 37

Avaya UCM role

Configuration and Orchestration Manager (COM) supports the following Avaya Unified Communications Management (UCM) user roles:

- NetworkAdministrator
- UCMSystemAdministrator
- UCMSuperOperator

The following table outlines the functions of the UCM user roles on UCM and COM components.

Table 6: UCM user roles on UCM and COM components

Component	NetworkAdministrator	UCMSystemAdministrator	UCMSuperOperator
Main Page	Yes	Yes	Yes
Security Management Page (Quantum Page)	Yes (users, roles, sessions, and policies management)	Yes (can only change the user password)	Yes (can only change user password)
Device and Server	Yes (read and write)	Yes (read only)	Yes (read only)

Component	NetworkAdministrator	UCMSystemAdministrator	UCMOperator
Credentials Page			
Backup and Restore Commands (no UI; only runs from the command line)	Yes (the OS user must be in the Administrators or root group)	Yes (the OS user must be in the Administrators or root group)	Yes (the OS user must be in the Administrators or root group)
License Page	Yes	Yes	Yes (read only)

The following table outlines the functionality of different UCM roles on COM.

Table 7: Functionality of UCM roles on COM

Functionality	Full or Node-based application license /UserRole =NetworkAdministrator (default admin user)	Full or Node-based application license / UserRole =UCMSystemAdmin	Full or Node-based application license /UserRole =Operator
Dashboard with topology	Yes	Yes	Yes
Device View (Inventory grid)	Yes	Yes	Yes
Discovery	Yes	Yes	No
EDM Plugin management	Yes	Yes	No
Plugin Launch	Yes	Yes	Yes
User Management	Yes	No	No
Device Group Manager	Yes	Yes	No
MEM assignment to User	Yes	Yes	No
MEM Usage (includes VRF Manager)	Yes	Yes	Yes, if access has been allowed to a specific MEM.
Device and Server Credentials Page	Yes	No	No

Functionality	Full or Node-based application license / UserRole = Network Administrator (default admin user)	Full or Node-based application license / UserRole = UCMSysAdmin	Full or Node-based application license / UserRole = Operator
SysLog, Traps Configurations	Yes	Yes	No
SysLog / Trap Viewers	Yes	Yes	Yes
Application Logs	Yes	Yes	Yes
Trouble Shooting Tools	Yes	Yes	Yes
Global Preferences	Yes	Yes	No
Backup and Restore Commands (no UI; only runs from the command line)	Yes	Yes	No
Wizard, template and scheduler	Yes	Yes	Yes, if access to a relevant manager has been provided.

Viewing existing users

Perform the following procedure to view the users who are configured for UCM access.

Procedure steps

1. In the Navigation pane, expand **Admin**, and then click **User Management**.

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

Administrative Users

Select a User ID to manage the properties and roles of local and externally authenticated users. Refer to password and authentication server policies for additional configuration requirements. Refer to [Active Sessions](#) for currently logged in users and session management functions.

Add... Reset

<input type="checkbox"/> User ID ▲	Name	Roles	Type	Account Status
1 <input type="checkbox"/> admin	Default security administrator	NetworkAdministrator	Local	Enabled
2 <input type="checkbox"/> siberiaadmin	sibaadmin	UCMSystemAdministrator	Local	Enabled
3 <input type="checkbox"/> siberiaop	siberiaop	UCMOperator	Local	Enabled

2. View the information for existing users.

Adding a new local or external user

Perform the following procedure to create a new user of UCM and to assign roles to the new user.

Procedure steps

1. In the Navigation pane, expand **Admin**, and then click **User Management**.
The Administrative Users page lists users configured for access to UCM.

Administrative Users

Select a User ID to manage the properties and roles of local and externally authenticated users. Refer to password and authentication server policies for additional configuration requirements. Refer to [Active Sessions](#) for currently logged in users and session management functions.

Add... Reset

<input type="checkbox"/> User ID ▲	Name	Roles	Type	Account Status
1 <input type="checkbox"/> admin	Default security administrator	NetworkAdministrator	Local	Enabled
2 <input type="checkbox"/> siberiaadmin	sibaadmin	UCMSystemAdministrator	Local	Enabled
3 <input type="checkbox"/> siberiaop	siberiaop	UCMOperator	Local	Enabled

2. Click **Add**.

Add New Administrative User

Step1: Identify the new user.
Enter the user's full name and select an authentication type and User ID. Locally authenticated users also require a temporary password.

User ID: (1-31) (Allowed characters are a-z, A-Z, 0-9, - and _)

Authentication Type: Local
 External

Full Name:

Temporary password:

Re-enter password:

The user will be required to change this password when logging in.

Allowed characters in the password are: a-zA-Z0-9!@#%&*+!?!; The length of your password must be at least 6 characters.

Note: The new user must be saved before you may assign roles.

3. In the **User ID** field, enter the user ID.
4. For the **Authentication Type** choose one of the following types:
 - 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. After the new user logs on to UCM for the first time, the user must change this password. Therefore, Avaya recommends that users record the new password in a secure place.

7. In the **Re-enter password** field, reenter the temporary password, and then click **Save and Continue**.

Add New Administrative User

Step2: Assign Role(s)

Selected roles authorize the user for associated features and element permissions.

Roles

<input type="checkbox"/>	Role Name	Elements	Description
<input type="checkbox"/>	MemberRegistrar		Member Registrar Role
<input type="checkbox"/>	NetworkAdministrator	All elements of type: Device Credential Admin All elements of type: Licensing Admin All elements of type: com All elements of type: Base OS All elements of type: Hyperlink	Network Administrator Role
<input type="checkbox"/>	Patcher		Patcher/PDT Role
<input type="checkbox"/>	UCMOperator	All elements of type: UCM Roles	UCM Operator

8. In the Role Name column, select the check boxes for the role that you want to assign to the user.
9. Click **Finish**.

The new user appears in the users list.

! Important:

The valid users are Network administrator, UCM System Administrator, and UCM operator.

Variable definitions

Variable	Value
User ID	User identification. This field accepts up to 31 characters, and allows characters such as lowercase letters (a–z), uppercase letters (A–Z), numbers (0–9), and special characters (- and _).
Authentication type	Type of user. Local user or External user.
Full Name	Full name of the user.
Temporary password	New password for the user. This field allows characters such as lowercase letters (a–z), uppercase letters (A–Z), numbers (0–9), and special characters ({} ()<>./.=[]_@!\$%~+":?'\;). The minimum length of the password is 8 characters.
Re-enter password	Reenter the new password for the user.
Role Name	Roles that a new user can perform.

Disabling a user

Perform the following procedure to disable a user in the UCM network.

Procedure steps

1. In the Navigation pane, expand **Admin**, and then click **User Management**.

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

Administrative Users

Select a User ID to manage the properties and roles of local and externally authenticated users. Refer to password and authentication server policies for additional configuration requirements. Refer to [Active Sessions](#) for currently logged in users and session management functions.

Add Disable Delete

User ID	Name	Roles	Type	Account Status
<input type="checkbox"/> 1 admin	Default security administrator	NetworkAdministrator	Local	Enabled
<input type="checkbox"/> 2 siberiaadmin	sibaadmin	UCMSystemAdministrator	Local	Enabled
<input type="checkbox"/> 3 siberiaop	siberiaop	UCMOperator	Local	Enabled

- In the User ID column, select the check box for the user you want to disable, and then click **Disable**.

The Account Status for the user you selected changes to Disabled.

Deleting a user

Perform the following procedure to delete a user in the UCM network.

Procedure steps

- In the Navigation pane, expand **Admin**, and then click **User Management**.

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

Administrative Users

Select a User ID to manage the properties and roles of local and externally authenticated users. Refer to password and authentication server policies for additional configuration requirements. Refer to [Active Sessions](#) for currently logged in users and session management functions.

Add Disable Delete

User ID	Name	Roles	Type	Account Status
<input type="checkbox"/> 1 admin	Default security administrator	NetworkAdministrator	Local	Enabled
<input type="checkbox"/> 2 siberiaadmin	sibaadmin	UCMSystemAdministrator	Local	Enabled
<input type="checkbox"/> 3 siberiaop	siberiaop	UCMOperator	Local	Enabled

- In the User ID column, select the check box for the user you want to delete, and then click **Delete**.
- After you are prompted to confirm the deletion of user, click **Delete**.

! Important:

Users cannot delete their own account.

Chapter 7: Licensing

This chapter provides information about adding a license file, exporting a license file, generating a license report, and refreshing license information.

Navigation

- [License restriction](#) on page 39
- [Node based licensing for COM](#) on page 39
- [Adding a license](#) on page 40
- [Exporting a license](#) on page 41
- [Generating a licensing report](#) on page 41
- [Refreshing the license information](#) on page 42

License restriction

Although you may discover more than licensed devices, you can only manage the devices you select. You can select the devices you want to manage from the pop up window that appears, or you can select multiple devices from the topology map, and right-click to select manage. After you select the devices, you must submit the devices.

Node based licensing for COM

Configuration and Orchestration Manager (COM) supports node based licensing that permits COM to manage the number of devices that you purchase a license for. An Enterprise license is available which provides COM 1500 node count support and a packaged Bulk Configuration Manager (BCM) base license.

After each discovery, you must select managed devices. Only the licensed number of devices are available to COM. The unselected devices are discarded. After a new discovery, you can change the device selection.

*** Note:**

If you upgrade COM from an earlier version, you must acquire a new COM 3.0.1 base license, because COM 2.3 base or earlier license files do not permit access to COM. However, upgrade licenses are valid between releases and work on COM 3.0.1.

Use the following table to determine whether or not you require a new license to upgrade to Avaya Configuration and Orchestration Manager (COM) 3.0.1 from an earlier version.

Old release installed	Server type	New license required
2.3 or 2.3.x	Physical machine	Yes
2.3 or 2.3.x	VMWare virtual machine	Yes
2.3 or 2.3.x	Non VMWare virtual machine	Yes
3.0	Physical machine	No
3.0	VMWare virtual machine	Yes
3.0	Non VMWare virtual machine	No

The following list outlines the types of COM node based licenses:

- COM_50_base—This is the base license in node-based licensing; manages 50 nodes only.
- COM_Upgrd50_250_base—This is an upgrade from a 50 to 250 nodes; manages 250 nodes only.
- COM_Upgrd50_1200_base—This is an upgrade from a 50 to 1200 nodes; manages 1200 nodes only.
- COM_Upgrd250_1200_base—This is an upgrade from 250 to 1200 nodes; manages 1200 nodes only.
- COM_Upgrd1200_1500_base—This is an update from 1200 to 1500 nodes; manages 1500 nodes only.

! Important:

You can combine any of the preceding licenses. However, you cannot have a 50_base and then a 250_1200_base license. The upgrade must go from 50 to 1200, or from 50 to 250 to 1200.

Adding a license

Perform the following procedure to add a license.

Procedure steps

1. In the Navigation pane, expand **Admin** panel, and then select **Licensing**.
2. From the Licensing Administration page, click **Add License**.
3. From the Add License dialog box, in the **License** field, browse to locate the license file.
4. Select the **License Host**, and then click **Add**.

Exporting a license

Perform the following procedure to export a license file.

Procedure steps

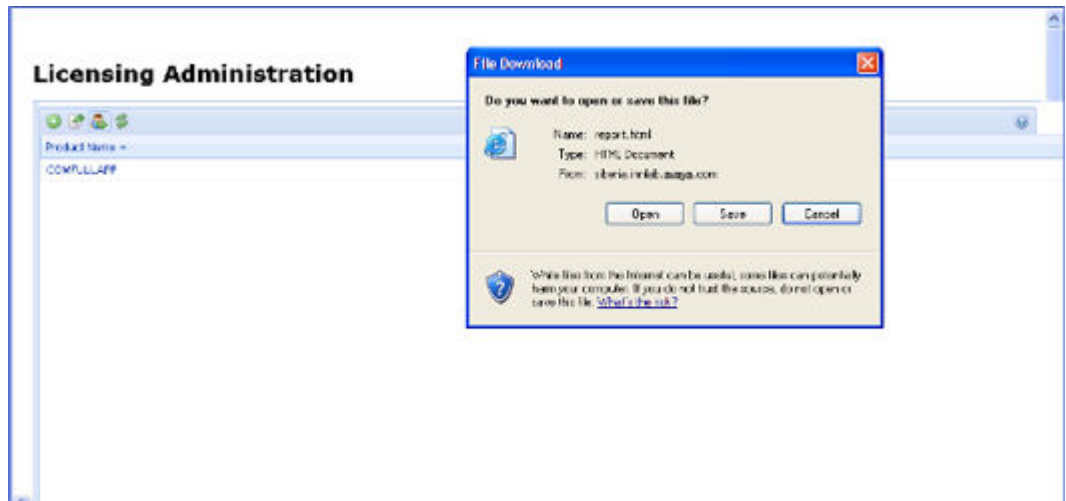
1. In the Navigation pane, expand the **Admin** panel, and then click **Licensing**.
2. From the Licensing Administration page, in the product name table, select the product license to be exported.
3. Click **Export License**.
4. In the File Download dialog box, click **Save**.

Generating a licensing report

Perform the following procedure to generate a licensing report.

Procedure steps

1. In the Navigation pane, expand the **Admin** panel, and then click **Licensing**.
2. From the Licensing Administration page, in the product name table, select the product license to be exported.
3. Click **Report**.



4. In the File Download dialog box, click **Save**.

Refreshing the license information

Perform the following procedure to refresh the license information.

Procedure steps

1. In the Navigation pane, expand the **Admin** panel, and then click **Licensing**.
2. From the Licensing Administration page, in the product name table, select the product license to be exported.
3. Click **Refresh**.

Chapter 8: Configuration and Orchestration Manager administration

This chapter provides information about how to administer Avaya Configuration and Orchestration Manager (COM).

Navigation

- [Access Control](#) on page 43
- [Preferences](#) on page 45
- [Device credentials](#) on page 54
- [User management](#) on page 31
- [Licensing](#) on page 39
- [Plugins inventory](#) on page 62
- [Audit log](#) on page 67

Access Control

The Access Control tab contains the MultiElementManager Assignment tab you use to assign Multi-Element Managers.

The Access Control service retrieves the role of the user from UCM-CS, and the access to other components is based on users role and licenses.

See the following sections to manage access control components.

- [Assigning MultiElement Manager](#) on page 43
- [Resetting MultiElement Manager assignment](#) on page 44
- [Clearing MultiElement Manager assignments](#) on page 45
- [Refreshing the available MultiElement manager list](#) on page 45

Assigning MultiElement Manager

Perform the following procedure to assign the MultiElement Manager to the selected Configuration and Orchestration Manager (COM) user.

Prerequisites

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

Procedure Steps

1. From the Navigation pane, expand the **Admin** pane, and then click **Access Control**.
2. From the MultiElement Manager Assignment tab, select a user.
3. In the **Multi-Element Manager Assignment** section, from the **Available MEM** list, do one of the following:
 - To assign one element manager, select the element manager that you want to assign, and then click the **Right Arrow**.
 - To assign several element managers, press and hold **Ctrl**, select the element manager, release **Ctrl**, and then click the **Right Arrow**.
 - To assign a contiguous block of element managers, press and hold **Shift**, select the first element manager and the last element manager, release **Shift**, and then click the **Right Arrow**.
 - To assign all the element managers, click the **Double right arrow**.
4. To remove one or more element managers, select them from the **Selected MEM** list, and then click **Left Arrow**.
To remove all the element managers, click **Double Left Arrow**.
5. Click **Apply**.

Resetting MultiElement Manager assignment

Perform the following procedure to reset the MultiElement Manager assignment for the selected Configuration and Orchestration Manager (COM) user.

Prerequisites

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

Procedure Steps

1. From the Navigation pane, expand the **Admin** pane, and then click **Access Control**.
2. From the MultiElement Manager Assignment tab, select a user.
3. Click **Reset**.

Clearing MultiElement Manager assignments

Perform the following procedure to clear the MultiElement Manager assignments for the selected Configuration and Orchestration Manager (COM) user.

Prerequisites

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

Procedure Steps

1. From the Navigation pane, expand the **Admin** pane, and then click **Access Control**.
2. From the MultiElement Manager Assignment tab, select a user.
3. Click **Clear User Assignments**.

Refreshing the available MultiElement manager list

Perform the following procedure to refresh the available MultiElement manager list.

Prerequisites

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

Procedure Steps

1. From the Navigation pane, expand the **Admin** pane, and then click **Access Control**.
2. From the MultiElement Manager Assignment tab, select a user.
3. Click **Refresh**.

Preferences

The Preferences option manages a set of Configuration and Orchestration Manager (COM) server preferences. For more information about discovering devices and configuring general and logging preferences, see the following sections.

- [Data persistence for COM managers](#) on page 46
- [Configuring a network discovery](#) on page 47
- [Scheduling a discovery](#) on page 48

- [Configuring general system preferences](#) on page 49
- [Configuring logging information](#) on page 50

Data persistence for COM managers

You can save the discovery information for managers into the database, and reload the discovery information for managers when a manager is opened.

Enabling the data persistence feature for COM managers

The manager discovery data is saved in MySQL database in the form of serialized Java objects, and uses the existing DeviceDataPersistence interface which is currently used to keep the discovery data in the memory as stateful session beans.

To enable or disable the database persistence feature, you must use the global preference Cache Manager Data. By default the feature is disabled. When the feature is disabled, the workflow of manager discovery and configuration is unchanged.

When you enable the database persistence feature, a warning message pops up. The message explains how the database persistence works and only recommends it for a static network.

The manager data in the database is identified by user and manager; for example, the same user can only have one copy of the manager data for each manager.

After you launch a manager, if there is no data saved in the database, a regular discovery begins. At the end of the discovery, the discovery information is automatically saved into the database.

When there is persistence data saved in the database, at the beginning of launching a manager, you are asked if you want to use the old persistence data, and are warned that you might not get the latest information from the network. If you select yes, the persistence data is loaded into the manager without a new discovery.

When you try to add, modify, or delete configurations within a manager, the manager sends the configuration changes to the devices and, if successful, saves the serialized DeviceDataPersistence Java object into the database to keep the database synchronized with the network.

There is no Save button for database persistence. All database saves happens automatically.

The following is the list of managers that support database persistence:

- MLT Manager
- VLAN Manager
- Routing Manager

Configuring a network discovery

You can configure the Configuration and Orchestration Manager (COM) application to perform a discovery to manage devices on your network. The discovery preferences that you set can determine the type of discovery the system performs and the landing page the system uses to display discovery results. Configuration and Orchestration Manager uses the information that you configure to discover devices and to create a topology map or an inventory grid.

You have the option to launch a new or merged network discovery. The new or merged discovery creates or updates the topology map or inventory grid, respectively.

Perform the following procedure to configure a network discovery.

Procedure steps

1. From the Navigation pane, open **Admin**, and then select **Preferences**.
Or
Navigate to the **Home** tab tool bar, and click **Set Discovery Preferences**, represented by a wrench.
2. Specify whether you want to configure a new or merged discovery:
 - **New discovery**—Run a new discovery when you want to introduce a device to your network.
 - **Merged discovery**—Run a merged discovery when you want to amend your device inventory without a new discovery.
3. In the **New Discovery Seed IP Address(es)** field, enter the IP address of one, or more than one, device in the network.
Separate multiple IP addresses with a comma.
4. In the **Max Hops** field, enter the maximum number of hops.
5. Choose a landing page by selecting the corresponding **Landing Page** option.
The default value is set to Topology. If you select the Inventory value, you are directed to the device inventory grid at log in.
6. Select the **Discover IP Phones** check box to discover the IP phones and to appear in the topology map.
7. Select the **Discover Unsupported Devices** check box to enable discovery of unsupported devices.
8. Select the **Save topology layout across discovery** check box to save the topology map.
9. Select the **Restrict Discovery** check box to restrict device discovery to only the devices entered in the subnets.

In the IP Address/addrLen dialog box, perform one of the following procedures:

- Click **Insert** to enter IP addresses.
 - Click **Delete** to delete IP address.
10. Click **Save Preferences** or **Save and Run Discovery**.

Scheduling a discovery

You can configure the Configuration and Orchestration Manager (COM) application to run scheduled network discovery jobs. You can set your discovery launch to occur one time, or repeatedly according to specific months, days of the week, date, and time. By scheduling your discovery event, you can run the discovery process without manual intervention. You also can schedule the discovery process to occur during off hours, therefore freeing up network resources.

Perform the following procedure to schedule a network discovery.

Procedure

1. From the Navigation pane, open **Admin**, select **Preferences**, and from the Discovery tab, click **Schedule Discovery**.
Or
Navigate to the Home tab tool bar, and select **Discover Topology > Schedule a Discovery**.
2. In the **Task Name** field, enter a value to identify the task name.
3. In the **Schedule Name** field, enter a value to identify the discovery schedule.
4. In the Schedule section, select one of the following scheduling interval options:
 - One Time Only
 - Every Month on The: x Day.
 - Every Week on: x
 - Every: x Days.
 - Every Day.
5. In the Date section, specify the starting date and time values for the scheduled event in the **Date** and **Time** fields.
6. Click **Set**.

Next steps

You can manage a scheduled discovery event on the View Scheduled Task tab. You have the option to delete, stop, reschedule, or run a scheduled discovery event.

Clearing a discovery

Perform the following procedure to clear a discovery. If you clear a discovery, you clear all the devices in the topology map.

Procedure

1. From the COM Navigation pane open **Admin**, and then click **Preferences**.
 2. From the Discovery tool bar, click **Clear Discovery**.
 3. Click **Yes**.
-

Viewing a discovery log

Perform the following procedure to view a discovery log.

Procedure

1. From the COM Navigation pane, open **Admin**, and then click **Preferences**.
 2. From the Discovery tab tool bar, click **View Discovery Log**.
 3. Select **Open with** or **Save File** to open the COM Discovery log.
 4. Click **OK**.
-

Configuring general system preferences

Perform the following procedure to configure the general system preferences.

Procedure

1. From the Navigation pane, open **Admin**, and then select **Preferences**.
2. Click the **General** tab.
3. As appropriate, enter field values in the following panes:
 - **SNMP**
 - **Database Clean-up**
 - **TFTP/SFTP**
 - **Manager**

- **Email Server**
 - **BCM Task Preference**
4. Click **Save Preferences**.

Configuring logging information

Perform the following procedure to configure logging.

Procedure steps

1. From the Navigation pane, open **Admin**, and then select **Preferences**.
2. Click the **Logging** tab.

The screenshot shows the 'Logging' tab in the 'Preferences' dialog. The 'Audit Log' section is expanded, showing the following settings: Audit Log File Size is 10 MB; Audit Log Level is INFO; Audit Log No Files is 3; Purge logs older than is 6 months. There are two radio buttons: 'Archive audit logs before purging to: C:/Program Files/Avaya/UCM/COM/log/Audit_Archives' (unselected) and 'Delete Permanently' (selected). An 'Archive Audit Logs now' button is present. The 'Debug Log' section is also expanded, showing: Debug Log File Size is 10 MB; Debug Log Level is ALL; Trace is unchecked; Debug Log No Files is 3. A 'Save Preferences' button is located at the bottom of the dialog.

3. Enter information in all the fields in the Logging dialog box as appropriate.
4. Click **Save Preferences**.

Job aid

The following table describes the fields in the Preferences tabs.

Table 8: Preferences fields

Tab/Panel	Item	Description
Discovery	Discovery Mode	The options are: <ul style="list-style-type: none"> • New • Merge
	Discovery Seed IP Address(es) (comma separated) For New or Merge Discovery mode.	The IP addresses of one or more devices that COM queries using SNMP to start the discovery process. For more information about supported devices, see <i>Avaya Configuration and Orchestration Manager Administration</i> (NN47226-600). <p>! Important:</p> If the devices you want to monitor and configure are not connected to the same network, you can specify multiple seed addresses, separated by commas. Separate networks do not appear to be connected in the network topology map.
	Max Hops [1–20]	The number of hops, between 1 and 20, that a data packet travels from one router or intermediate point to another in the network. The default value is 5 hops.
	Landing Page	The options are: <ul style="list-style-type: none"> • Topology • Inventory
	Discover IP Phones	If selected, IP phones are discovered and appear in the topology map.
	Discover Unsupported Devices	If selected, unsupported devices are discovered and appear in the topology map.
	Save topology layout across discovery	If selected, COM saves the topology layout across discovery.
	Restrict Discovery	Opens the Restrict Discovery dialog box to restrict device discovery to only the devices in the subnets entered.
General SNMP panel	Retry Count [0..5]	The number of times, between 0 and 5, that COM tries to connect to a device using SNMP. The default value is 1.
	Timeout [3..120 seconds]	The amount of time, between 3 and 10 seconds, that COM waits before trying to connect to a device again. The default value is 5.

Tab/Panel	Item	Description
	Max Outstanding Requests[20..250]	The number of SNMP requests, between 20 and 250, that COM maintains as open or outstanding. The default value is 100.
	Listen for Traps	If checked, COM receives traps for all the devices managed through COM.
	Listen for Syslogs	If checked, COM receives logs for all the devices managed through COM.
	Trap Listener Port[1–65535]	The port on the COM server where the COM software listens for traps.
	System Log Listener Port[514..530]	The port on the COM server where the COM software listens for syslogs.
	Trap Poll Interval[5..60 min]	The trap poll interval is associated with the trap parser in the Trap Viewer Manager. As you build a parser, you can select to have devices automatically highlighted on the topology map after the trap is received in the database. The poll interval informs the browser how often to go to the database to look for traps that have come in. The values are 5 minutes to 60 minutes.
General Database Clean-up panel	Trap/Syslog Storage (days) [1..365]	The number of days, between 1 and 365, that COM tries to connect to Trap/Syslog storage to purge the database. The default value is 90.
	Trap/Syslog Check Time (Hour)[0..23]	The number of hours, between 0 and 23, that COM tries to connect to a storage to purge the database. The default value is 1.
	Trap/Syslog Check Time (Min.)[0..59]	The number of times, between 0 and 59, that COM tries to connect to a storage to purge the database. The default value is 0.
	Trap/Syslog Check Frequency (days) [1..30]	The number of days, between 1 and 365, that COM tries to connect to Trap/Syslog storage to purge the database. The default value is 90.
General TFTP/SFTP panel	TFTP/SFTP Server	Allows you to enter the IP address of the default TFTP or SFTP server used by submanager applications.
General Manager panel	Cache Manager Data	Applies only to the MultiLink Trunking Manager, Routing Manager, and VLAN Manager, and is optional. If you check the Cache Manager Data check box, you permit the managers to cache the device data that the managers discover the first time. Therefore, if you reopen the managers, COM does not perform another discovery, but displays the data

Tab/Panel	Item	Description
		from the first discovery. Avaya recommends that you use this feature for very static networks only. If you check the Cache Manager Data check box, a dialog box appears to explain the feature and ask you if you want to proceed.
General EMail Server	SMTP Host	The name of the SMTP host.
	SMTP User Name	The SMTP user name.
	SMTP Password	The SMTP password.
	From User	The e-mail address of the sender.
	To Recipient	The e-mail address of the recipient.
	Port	The port number.
	Enable Email	If checked, enables the e-mail function.
	Test Email	Click to test the EMail server.
General BCM Task Preference	BCM Task Concurrent Device Operations Limit 1–10	Controls the maximum number of concurrent operations on devices running in a task. The values are 1 to 10.
Logging Audit Log	Audit Log File Size [Example, 10 KB 10 MB 10 GB]	You can specify the Audit Log File Size. The default value is 10 MB.
	Audit Log Level	You can specify the Audit Log Level. The default value is INFO.
	Audit Log No Files[1–10]	The number of files which are audited. The default value is 3.
	Purge logs older than	You can specify the length of time audit logs remain in the database before they are archived, in weeks or months. The default value is 6 months.
	Archive audit logs before purging to	If selected, you can specify the location to save the audit log backup file, in CSV format.
	Delete Permanently	If selected, deletes audit log files without creating backup files
Logging Debug Log	Debug Log File Size [Example, 10 KB 10 MB 10 GB]	You can specify the Debug Log File Size. The default value is 10 MB.
	Debug Log Level	You can specify the Debug Log Level. The default value is ALL.
	Trace	If checked, additional SNMP information is written to the COM error log, and can provide assistance in troubleshooting.

Tab/Panel	Item	Description
		<p>! Important: Selecting Trace can slightly slow down performance as extra information is gathered</p>
	Debug Log No Files[1–10]	The number of files which are debugged. The default value is 3.

Device credentials

The credentials service provides the necessary data to connect to a device, and can store credentials for the following protocols:

- SNMPv1/v2
- SNMPv3
- Telnet
- Common Information Management (CIM)
- Secure Shell (SSH)
- Netconf
- File Transfer Protocol (FTP)
- RLogin
- Windows User

Configuration and Orchestration Manager (COM) requires that you enter either SNMPv1/2 or SNMPv3 credentials. If you enter SNMPv3 credentials, the credential must be mapped to a management user. Configuration and Orchestration Manager also requires that you enter telnet credentials for the FIM module. The Bulk Configuration Manager (BCM) module within COM requires either Telnet and SSH credentials to be available.

The following table lists the categories of credential information that COM manages in the Device and Server Credentials Editor.

Table 9: Device and Server Credentials Editor fields

Credential information	Attributes
Set Name	Credential set name.
IP Address or Range	Device/Server IP Address or Address Range.
SNMPv1/v2	Read Community Write Community.

Credential information	Attributes
SNMPv3	SNMPv3 User Authorization Protocol (MD5, SHA1, None) Authorization Key Privacy Protocol (AES128, DES, 3DES, None) Privacy Key.
Telnet	Telnet User name Telnet Password Telnet Port.
CIM	CIM User name CIM Password.
SSH	SSH User name SSH Password SSH Port.
NetConf	NetConf User name.
FTP	FTP User name FTP Password FTP Port.
RLogin	RLogin User name RLogin Password.
Windows User	Windows User name Windows Password Windows Domain.

Navigation

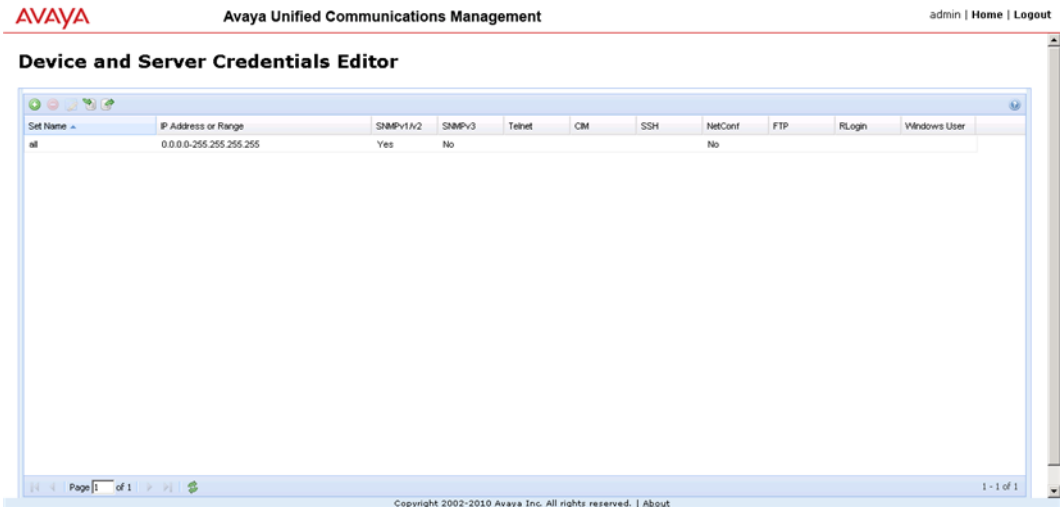
- [Adding a credential set](#) on page 55
- [Adding a credential set for SNMPv3](#) on page 57
- [Deleting a credential set](#) on page 58
- [Editing a credential set](#) on page 59
- [Importing a credential set](#) on page 60
- [Exporting a credential set](#) on page 61

Adding a credential set

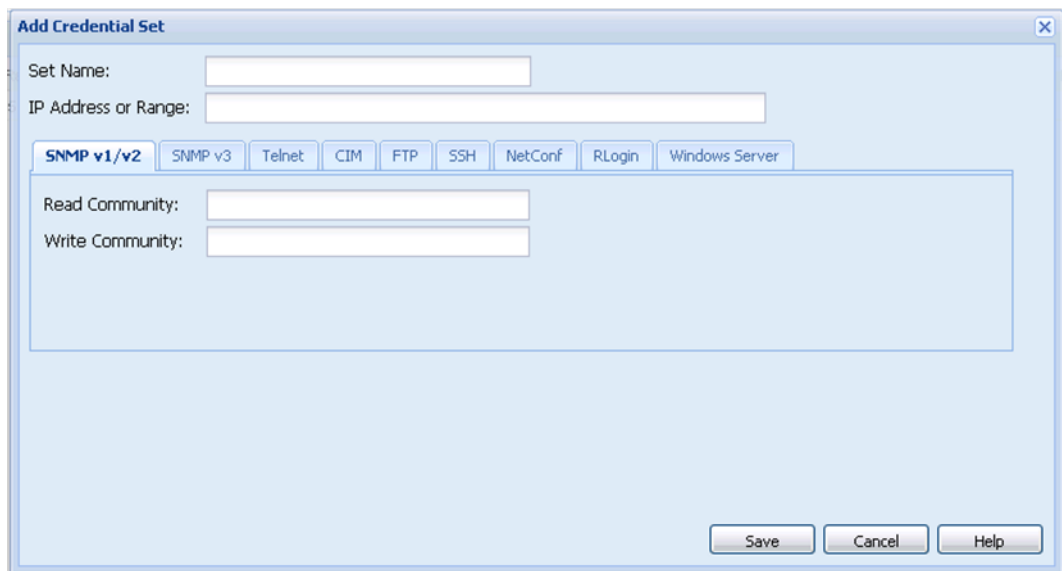
Perform the following procedure to add a new credential set to Unified Communications Management (UCM). You must add a credential set for each device you want to manage. The set name accepts printable ASCII characters, but not special characters (%(!)). You can enter the space (), dash (-), and underscore (_) characters. The set name must be unique. If you add a new entry or rename an existing one with a set name already used in another entry, a warning message appears.

Procedure steps

1. In the Navigation pane, expand **Admin**, and then click **Device Credentials**.



2. Click **Add Credential**.



3. In the **Set Name** field, enter the Set Name.
4. In the **IP Address/Range** field, specify the IP address information for the credential.
5. Add device credential information on the appropriate tab. For more information about the available tabs, see [Table 9: Device and Server Credentials Editor fields](#) on page 54.

Each tab corresponds to an authentication protocol. The information you enter depends on the type of authentication your device uses.

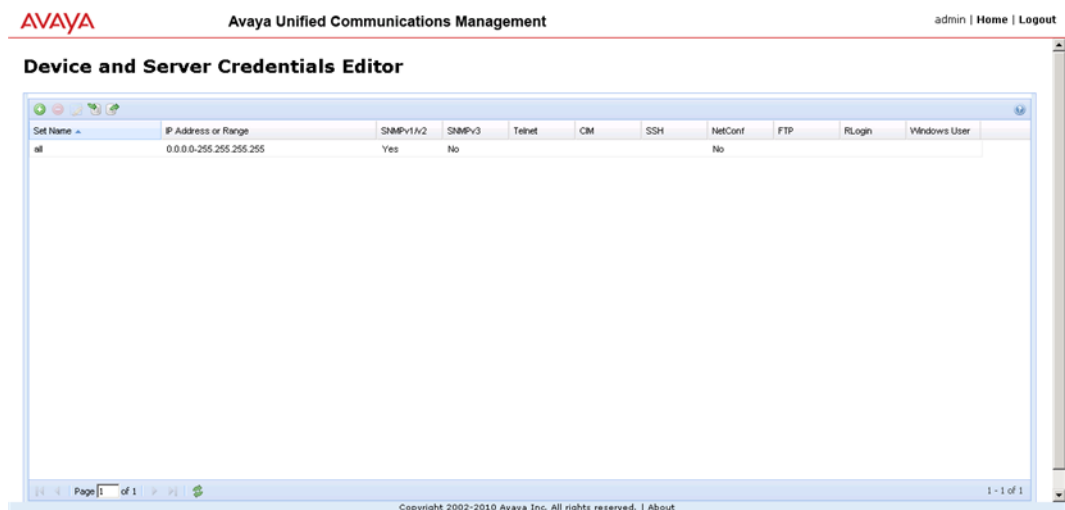
6. Click **Save**.

Adding a credential set for SNMP v3

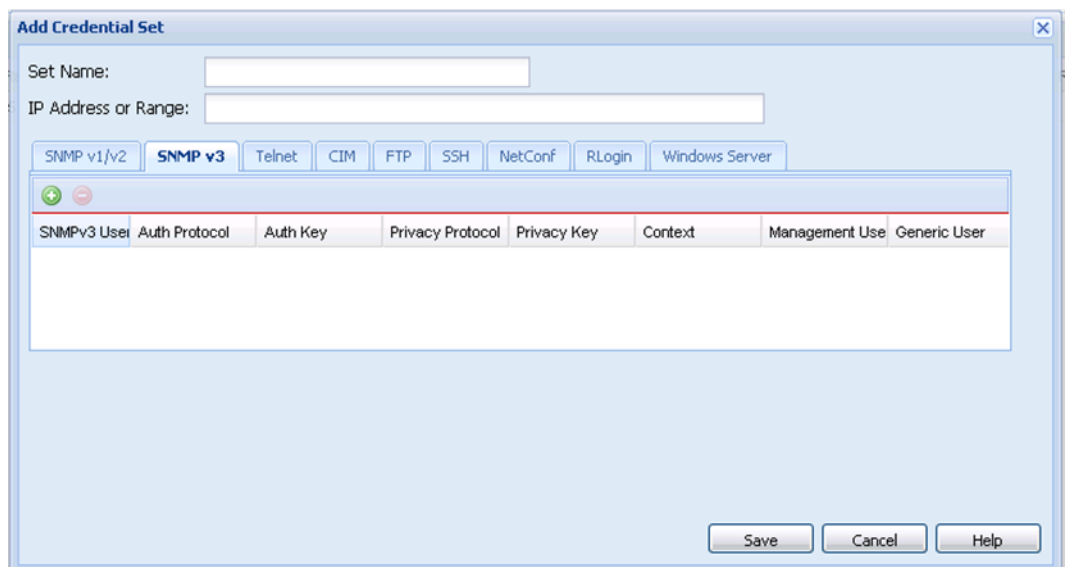
Perform the following procedure to add credentials for SNMP v3.

Procedure steps

1. In the Navigation pane, expand **Admin**, and then click **Device Credentials**.



2. Click **Add Credential**.
3. In the **Set Name** field, enter the Set Name.
4. In the **IP Address/Range** field, specify the IP address information for the credential.
5. Click **SNMP v3**.



6. Click **Add User**.
7. Enter appropriate values for all the fields in the SNMP v3 tab. For the Context, Management User, and Generic User fields, follow the guidelines listed below:

Context—If there is a VRF assigned to this user the VRF number should be configured in Context field.

Management User—You must associate the device snmp v3 user to a UCM user, otherwise the entry will not take effect.

Generic User—Ensure this field is set to true.

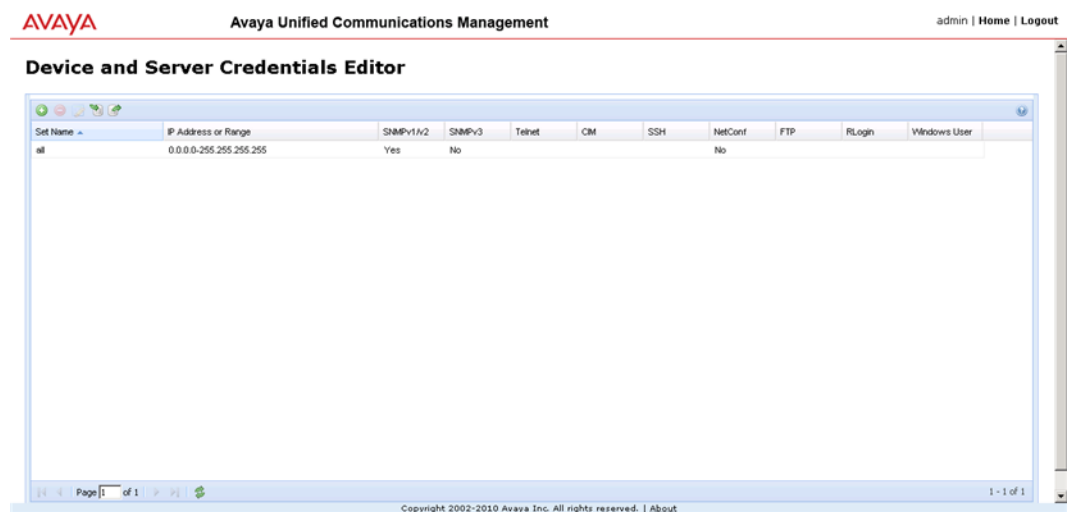
8. Click **Save**.

Deleting a credential set

Perform the following procedure to remove a credential set from the Device and Server Credentials Editor.

Procedure steps

1. In the Navigation pane, expand **Admin**, and then click **Device Credentials**.



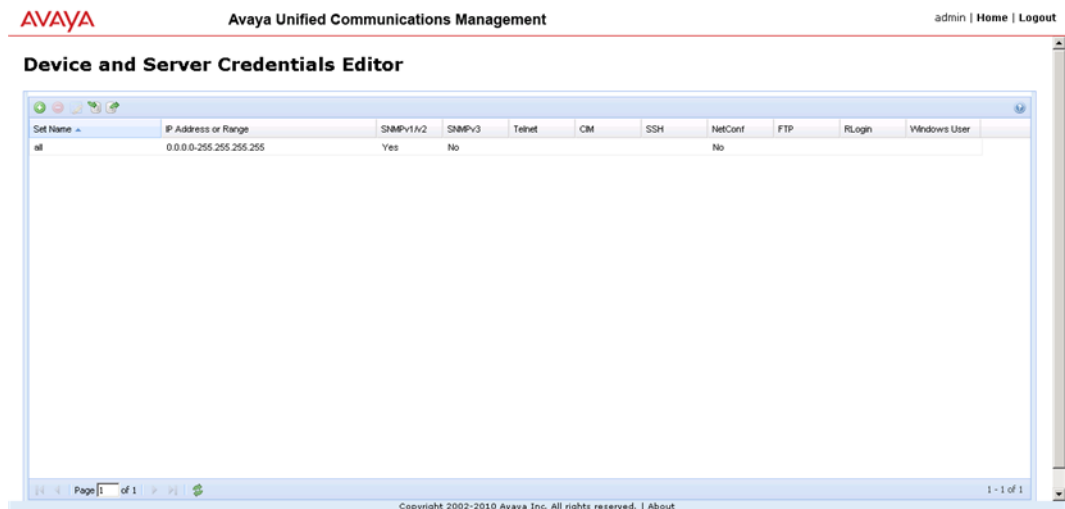
2. Click the credential set that you want to remove. You can select several credential sets at once by pressing **Ctrl**, and then clicking the credential sets.
3. Click **Delete Credential Set(s)**.
4. After you are prompted to confirm the deletion of the credential set, click **Delete**.

Editing a credential set

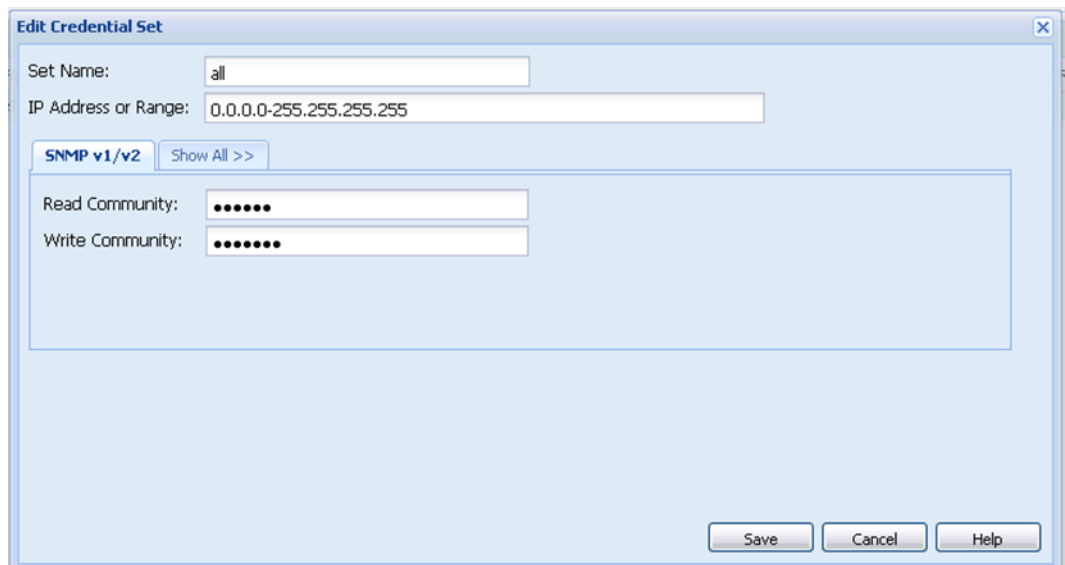
Perform the following procedure to edit a credential set to change the set name, IP address, and device credential information for a credential set.

Procedure steps

1. In the Navigation pane, expand **Admin**, and then click **Device Credentials**.



2. Click the credential set that you want to change.
3. Click **Edit Credential Set**.



4. Make changes to the credential set as required.

5. If you want to specify a different type of device credential information, click the **Show All** tab, and then type the new device credential information in the appropriate tab.
6. Click **Save**.

Unified Communications Management validates all specified IP addresses after saving the changes.

Importing a credential set

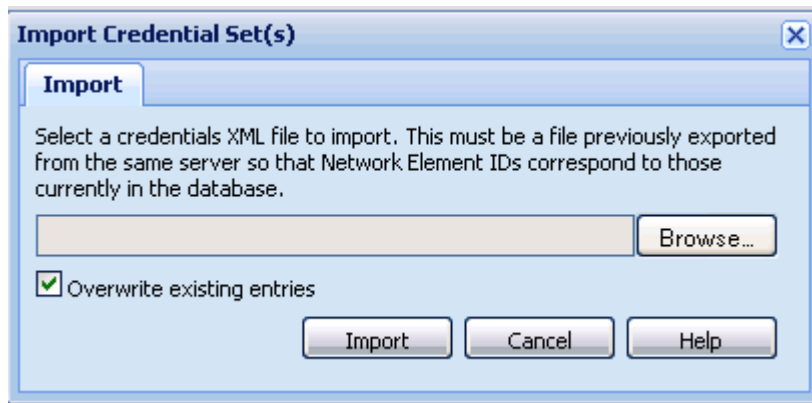
Perform the following procedure to import the credential set to Unified Communications Management (UCM).

Procedure steps

1. In the Navigation pane, expand **Admin**, and then click **Device Credentials**.



2. Click **Import Credentials**.



3. Click **Browse**, and then choose the credentials XML file to import.

4. To overwrite the existing entries of credential set, select the **Overwrite existing entries** check box.
5. Click **Import**.

Exporting a credential set

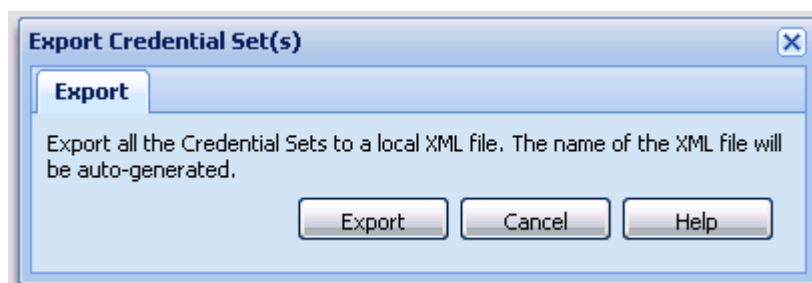
Perform the following procedure to export a credential set from the UCM to a local XML file.

Procedure steps

1. In the Navigation pane, expand **Admin**, and then click **Device Credentials**.

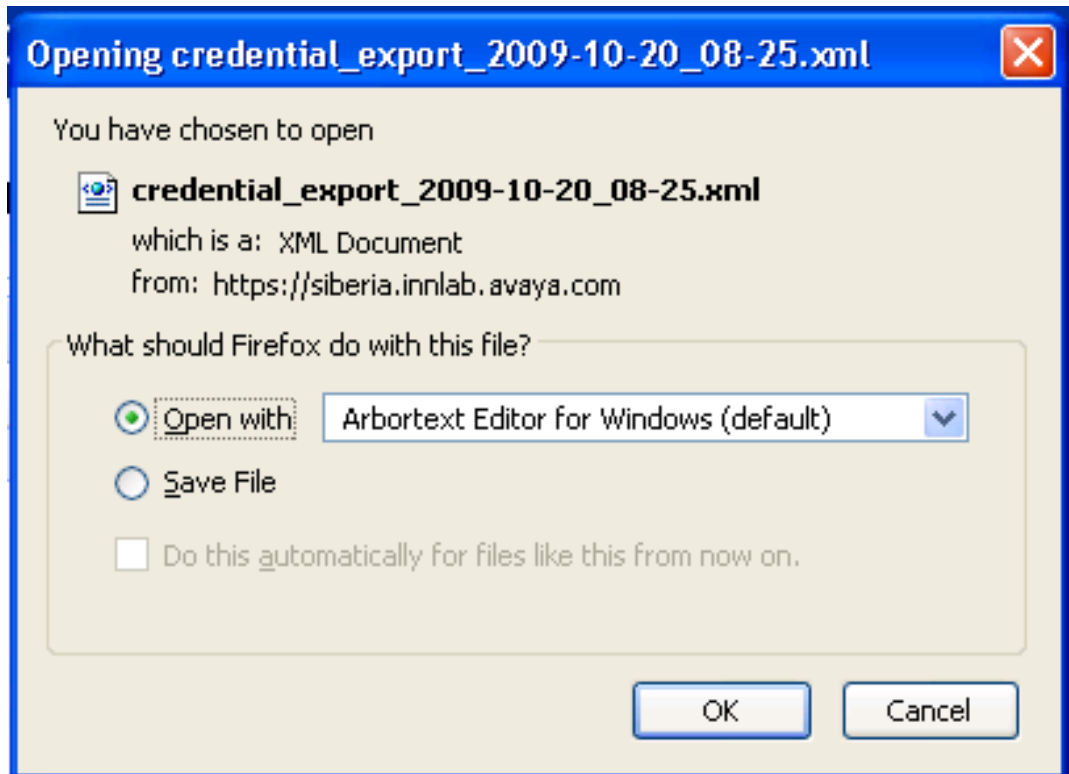


2. Click **Export Credentials**.



3. Click **Export**.

The Credential Sets exports to a local XML file. The name of the XML file is autogenerated.



4. Click **Save**.

Plugins inventory

The EDM plugin is a device plugin for a device version, or type, that you can install on an installed Configuration and Orchestration Manager (COM) base. You can install plugins on a Base or Complete application license. The user of the Network Administrator and UCM System Administrator roles can perform the Plugin management. You can install, uninstall, or view the EDM Plugin by accessing the Plugins Inventory.

EDM plugins offer device management capabilities. Therefore, if you want to perform QOS / Filters operation on a particular device, then you can manipulate this functionality from the Element Manager for this device. The Element Manager for the EDM plugins is a browser-based solution that is launched through the device inventory or from the topology map. To launch the Element Manager, right-click on a device. The EDM plugins are reused from the embedded EDM, or Element Manager, that is available in all the devices.

Configuration and Orchestration Manager displays the EDM Plugin Inventory with a table containing all the installed Plugins on the COM 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.

Navigation

- [Downloading EDM plugin](#) on page 63
- [Installing EDM plugin](#) on page 63
- [Uninstalling EDM plugin](#) on page 65
- [Refreshing the plugin inventory table](#) on page 65
- [Selecting the EDM preferences](#) on page 66

Downloading EDM plugin

Perform the following procedure to download an EDM plugin.

Note:

Use Firefox to download EDM plugin from the Avaya support site to the Configuration and Orchestration Manager (COM) server.

Procedure steps

1. Open a Web browser, and go to the Avaya support website: <http://support.avaya.com>.
2. Select the EDM Plugins section.
3. Download **EDM Plugin** for a specific device type and version.
4. Click **Save** to save the plugin file on to disk, where you are running the web-browser.

Installing EDM plugin

Perform the following procedure to install an EDM plugin on Configuration and Orchestration Manager (COM).

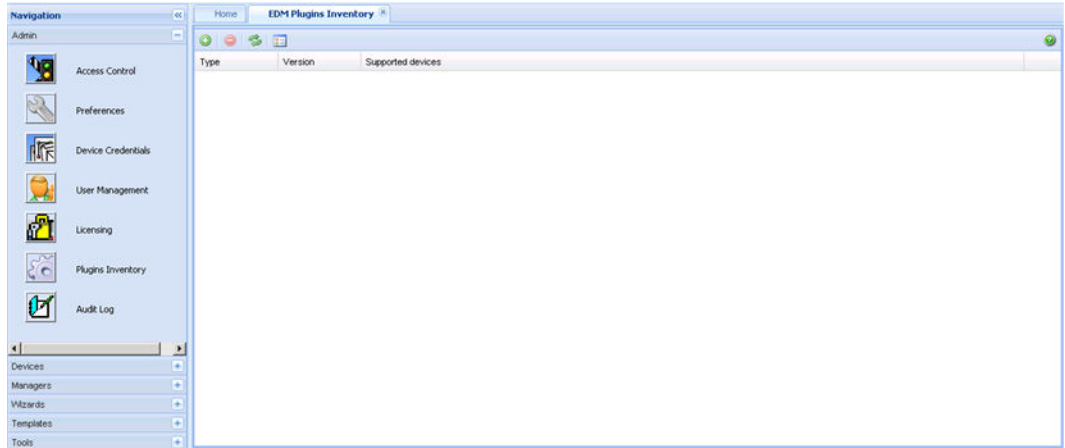
The installation process copies the file inside the JBoss deploy folder, adds the plugin related information in EDMsupportedDevices.xml file, which contains information about all the installed plugins, and copies the mib.dat file specific for the plugin at [COM_HOME]/dats/.

Prerequisites

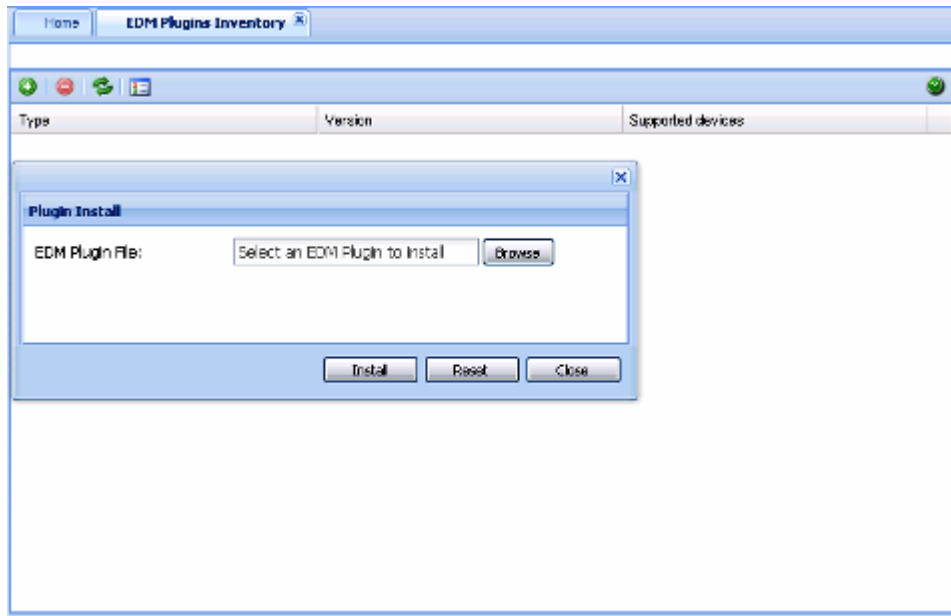
- You must have Network administrator role or UCM system administrator role rights to access the Plugins Inventory.
- Ensure that you log on to COM as an administrator.

Procedure Steps

1. Download **EDM plugin** using the procedure, [Downloading EDM plugin](#) on page 63.
2. From the Navigation pane, expand the **Admin** pane, and then click **Plugins Inventory**.



3. Click **Install Plugin**.



4. To select the EDM Plugin file, click **Browse**.
5. Browse to the EDM plugin file, and then click **Open**.
The file appears in the EDM Plugin File field.
6. To reset the EDM Plugin file, click **Reset**.
7. Click **Install**.

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

Uninstalling EDM plugin

Perform the following procedure to uninstall an EDM plugin from Configuration and Orchestration Manager (COM).

The uninstallation process deletes the war file from the JBoss deploy folder, removes information related to the plugin from the EDMsupportedDevices.xml file, and deletes the mib.dat file used by the plugin from [COM_HOME]/dats/.

Prerequisites

- You must have Network administrator role or UCM system administrator role rights to access the Plugins Inventory.
- Ensure that you log on to COM as an administrator.

Procedure Steps

1. From the Navigation pane, expand the **Admin** pane, and then click **Plugins Inventory**.
2. From the EDM Plugins Inventory table, select the plugin that you want to uninstall.
3. From the toolbar, click **Uninstall Plugin**.

If the uninstallation is successful, COM displays the following message: “EDM Plugin uninstall” successful. If the uninstallation is not successful, COM displays an error message that describes the problem.

Refreshing the plugin inventory table

Perform the following procedure to refresh the plugin inventory table.

Prerequisites

- You must have Network administrator role or UCM system administrator role rights to access the Plugins Inventory.
- Ensure that you log on to Configuration and Orchestration Manager (COM) as an administrator.

Procedure Steps

1. Download **EDM plugin** using the procedure, [Downloading EDM plugin](#) on page 63.
2. From the Navigation pane, expand the **Admin** pane, and then click **Plugins Inventory**.
3. From the toolbar, click **Refresh Plugin Inventory**.

Selecting the EDM preferences

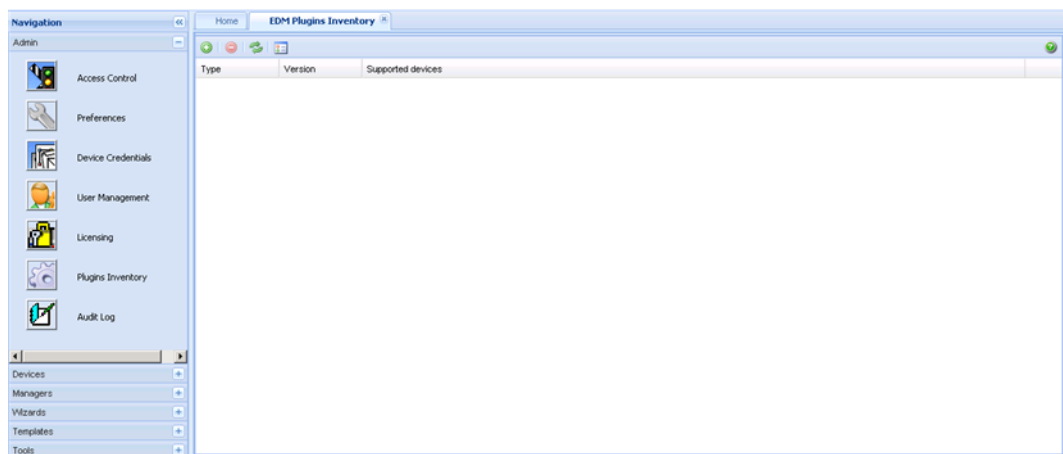
Perform the following procedure to use an EDM Plugin when launching the Single Element Manager.

Prerequisites

- You must have Network administrator role or UCM system administrator role rights to access the Plugins Inventory.
- Ensure that you log on to Configuration and Orchestration Manager (COM) as an administrator.

Procedure Steps

1. Download **EDM plugin** using the procedure, [Downloading EDM plugin](#) on page 63.
2. From the Navigation pane, expand the **Admin** pane, and then click **Plugins Inventory**.
3. From the toolbar, click **EDM Preferences**.



4. Select the check box for **Use EDM Plugin when launching Single Element Manager**.

By default the check box for Use EDM Plugin when launching Single Element Manager is selected.

! Important:

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

Click **Save**.

Audit log

All managers, including Topology and Discovery, send log messages to audit and debug logs. In the audit log, you can configure and perform the following audit log functions:

- print logs
- export logs
- filter logs
- refresh log listings
- generate log reports
- archive logs
- delete logs

For more information about configuring and using the audit log feature, see *Avaya Configuration and Orchestration Manager Administration* (NN47226-600).

Launching the audit log

Perform the following procedure to start the audit log.

Procedure steps

1. From the Navigation pane, expand the **Admin** panel.
2. Click **Audit Log**.

Audit Log Report Viewer tabs

The following table describes the Audit Log Report Viewer tabs.

Table 10: Audit Log Report Viewer tabs

Tab	Description
Date Time	The date and time at which the event occurred.

Tab	Description
Audit Level	The audit level of the audit message, for example INFO, ERROR, or WARNING.
User	The COM user name.
Access Type	The type of access to the device, for example read or write.
Source	The module name from which the log messages originate, for example, MultiLink Trunking Manager, Multicast Manager, Multimedia Manager, Routing Manager, Security Manager, Trap/Log Inventory, VLAN Manager, VPN Manager, Virtual Routing Manager, BCM, and COM.
Device IP	The corresponding IP address of the device.
Message	The audit message.

Chapter 9: Device inventory and group management

With the Device Inventory View, you can manage the Avaya Configuration and Orchestration Manager (COM) inventory. Configuration and Orchestration Manager provides a device inventory view of all the devices that are currently discovered in the network. You can sort the inventory list based on various device attributes.

This feature is included in the COM_50_base license.

You use the Device Group Manager to create and manage device and group assignments. You can use device groups to group a number of discovered devices from a single repository. You can use group assignments to control access to these grouped devices through context settings. The context setting defines device group accessibility for users based on their domain of responsibility. The context setting also determines whether device map topologies render for users at login.

For more information about configuring device inventory view, device group manager, and inventory manager, see *Avaya Configuration and Orchestration Manager Administration* (NN47226-600).

Navigation

- [Device Inventory View](#) on page 69
- [Device Group Manager](#) on page 70
- [Inventory Manager](#) on page 75

Device Inventory View

You can use the toolbar options on the Device Inventory View tab to manage devices on the inventory grid. For example, you can launch the element manager, and perform device actions such as pinging and viewing connections.

You also can use the Device Inventory View tab to draw a device topology from the inventory grid.

The following table lists and describes the Device Inventory View tool bar options available.

Table 11: Device Inventory View tool bar options

Option	Description
Perform Device Action	<p>Use this option to perform the following actions on a topology map device:</p> <ul style="list-style-type: none"> • Show Port Status—View port status. • Ping Device—Ping devices. • Show Properties—View device properties. • Dump Topology—View a topology dump. • Learned Mac Address—View learned MAC addresses. • Launch Element Manager—Open a new web page with the Element Manager for a device. • Administrative Actions—Perform the following administrative functions: <ul style="list-style-type: none"> - Update Device Topology - Change IP Address <p>You also can access these options through the right-click menu of a device on the topology map or inventory grid.</p>
Import/Export Inventory	Imports/Exports the inventory from, or to, a XML file.
Refresh	Refreshes the Device Inventory information.
Draw Topology	Use this option to create a network topology map from the inventory grid view.
Filter	<p>Filters the inventory view based on the following:</p> <ul style="list-style-type: none"> • Device Type • IP Address • Version • Name
Show All Inventory	Use this option to display all of the devices in the inventory as opposed to the ones in the device group.

Device Group Manager

You can use the toolbar options on the Device Group Manager tab to create and manage device and group assignments. For example, you can create device and user groups, edit devices or users in the individual groups, and highlight groups on a topology map.

You use device groups to group a number of discovered devices from the single repository. You then assign device groups to users. Each user can have multiple group assignments, but

only on context setting or device group. You can access the **Device Group Manager** tab by selecting the Device Group Manager icon in the Configuration and Orchestration Manager (COM) Navigation tree.

The following table lists and describes the Device Group Manager toolbar buttons in both the Devices and User Groups tabs.

Table 12: Device Group Manager toolbar options

Option	Description
Refresh	Use this option to refresh the device and user group view. The COM application communicates with the server to get the latest list of device and user groups.
Add Device Group or Add User Group	Use this option to add a device group or a user group. When you select the Add Device Group button, COM displays the Add Group window. When you select the Add User Group button, COM displays the Add Group window.
Delete Device Group or Delete User Group	Use this option to delete a device group or a user group from the system. You can delete a group only if the group is not associated to a user. If you delete a user group, the current context of the user is also removed from the system; no device list is displayed.
Apply Changes	Use this option to apply any changes that you make to the device group or user group.
Revert Changes	Use this option to revert any changes that you make to the device group or user group.
Highlight on Topology	Use this option to highlight a device group on the topology map.

Adding a device group

Perform the following procedure to add a device group using the Device Group Manager.

Before you begin

Ensure that you are logged on to Configuration and Orchestration Manager (COM) as a default admin.

Procedure

1. From the Navigation pane, expand **Devices**, and then click **Device Group Manager**.
 2. From the Groups toolbar, click **Add Device Group**.
 3. In the Add Group dialog box, enter a **Group Name**.
The Group Name field is required. Use letter, digit, underscore, or dash characters only.
 4. In the Devices section, select one or more than one device from the Available list, and then click the right-pointing arrow to move the devices to the Selected list.
 - To select all devices, click the double right-pointing arrow.
 - To remove a device, highlight a device from the Selected list, and click the left-pointing arrow.
 - To remove all devices, click the double left-pointing arrow.Use the Search field to locate a device from the Available list.
 5. Click **Save**.
-

Deleting a device group

Perform the following procedure to delete a device group in the Device Group Manager.

Before you begin

You must be logged on to Configuration and Orchestration Manager (COM) as an administrator.

Procedure

1. From the Navigation pane, expand **Devices**, and then click **Device Group Manager**.
 2. From the Groups table, select a group.
 3. From the Groups toolbar, click **Delete Device Group**.
 4. Click **Yes**.
-

Adding a user group

Perform the following procedure to add a user group in the Device Group Manager.

Before you begin

- You must be logged on to Configuration and Orchestration Manager (COM) as an administrator.
- You must have at least one administrative user assigned in the Avaya Unified Communications Manager (UCM) that is available for group assignment.

Procedure

1. From the Navigation pane, expand **Devices**, and then click **Device Group Manager**.
2. Click the **Group Assignments** tab.
3. From the Group Assignments toolbar, click **Add User Group**.

*** Note:**

An error message stating that all users have been associated with groups, indicates that there are no administrative users assigned in UCM that are available for group assignments.

4. In the **User** field, click the down arrow, and select a user.
5. In the **Current Context** field, click the down arrow to select a group.
6. In the Groups section, from the Available list, select one device, or more than one device, and click the right-pointing arrow to move the devices to the Selected list.
 - To select all devices, click the double right-pointing arrow.
 - To remove a device from the Selected list, select the device and click the left-pointing arrow.
 - To remove all devices from the selected list, click the double left-pointing arrow.

*** Note:**

You can use the Search field to select from the available list based on a complete or partial group name.

7. Click **Save**.
-

Editing a user group

Perform the following procedure to edit a user group in the Device Group Manager.

Before you begin

You must be logged on to Configuration and Orchestration Manager (COM) as an administrator.

Procedure

1. From the Navigation pane, expand **Devices**, and then click **Device Group Manager**.
2. Click the **Group Assignments** tab.
3. In the Group Assignments table, click a field in the Assigned Groups column.
4. In the **User** field, enter a user name.
5. In the Groups section, from the Available list, select one device, or more than one device, and click the right-pointing arrow to move the devices to the Selected list.
 - To select all devices, click the double right-pointing arrow.
 - To remove a device from the Selected list, select the device and click the left-pointing arrow.
 - To remove all devices from the selected list, click the double left-pointing arrow.

You can use the search field to search for a device in the Available list.

6. Click **Ok**.
 7. Click **Apply Changes**.
-

Deleting a user group

Perform the following procedure to delete a user group in the Device Group Manager.

Before you begin

You must be logged on to Configuration and Orchestration Manager (COM) as an administrator.

Procedure

1. From the Navigation pane, expand **Devices**, and then click **Device Group Manager**.
 2. Click the **Group Assignments** tab.
 3. Select a row, and click **Delete User Group**.
 4. Click **OK**.
-

Inventory Manager

Inventory Manager has two primary functions—file management and inventory management. With the Inventory Manager you can view the hardware and software configurations for different devices.

Use the Inventory Manager to perform the following actions for a device:







- view hardware configuration
- view software configuration
- edit Preferences
- download files from a device
- upload files to a device
- backup configuration files
- restore configuration files
- archive configuration files
- synchronize configuration files
- upgrade devices
- compare runtime configuration with existing configurations

For more information about Inventory Manager, see *Avaya Configuration and Orchestration Manager Administration* (NN47226-600).

Toolbar commands

The following table describes the Inventory Manager toolbar commands.

Table 13: Inventory Manager toolbar commands

Command	Toolbar button	Description
Reload / Discover		Rediscovered the inventory information and reloads the Inventory Manager with the latest information.
Find		Finds matching text strings in the navigation or contents panes.
Highlight on topology		Highlights devices of the selected family on the Configuration and Orchestration Manager (COM) topology map.
Preferences		Filters devices based on Family or Capabilities.
Export		Exports inventory information displayed in content panel grid in to a text file.
Help		Opens online Help for the current folder or tab.

Menu bar commands

The following table describes the Inventory Manager menu bar commands for the File menu and the Action menu.

Table 14: Inventory Manager menu bar commands for the File menu and the Action menu

Command	Menu	Description
Reload	File	Use to reload the manager from the Device Inventory View.
Save Inventory Info	File	Use to save inventory files that you can load again later.
Open Inventory File	File	Use to load saved inventory files.
Save Inventory in tab delimited text file	File	Use to save network inventory information in a tab-delimited text file.
Download file to Device(s)	Action	Use to download configuration or image files or both to devices.

Command	Menu	Description
Upload file from Device(s)	Action	Use to upload configuration or image files or both from devices.
Backup Config File	Action	Use to create backup files that can be restored to devices in the event of a network.
Save Backed Up Config Files to Local	Action	Use to view, download, or copy files from the COM server to your local desktop or PC. The backup files are always on the COM server. From a remote browser connection you can view the device files, or copy the device files locally.
Restore Config File	Action	Use to restore the configuration for the target device(s).
Archive Config File	Action	Use to archive the configuration for the target device(s).
Synchronize Config File	Action	Use to synchronize the configuration for the target device(s).
Device Upgrade	Action	Use to update the software for the specified device(s).
Device Upgrade Wizard	Action	Displays the Auto Upgrade form.
Compare Runtime Config With Existing Config	Action	Use to compare the runtime configuration for the specified device(s) with the external configuration file.

Chapter 10: Managers overview

Avaya Configuration and Orchestration Manager (COM) supports submanagers that provide detailed device information and management capabilities. The submanagers are designed to provide specialized information in an easy-to-use interface that is consistent in layout across the submanagers. A submanager can query COM and instruct the primary application to update the topology view with information relevant to the submanager view. For example, VLAN Manager can instruct COM to highlight all the devices in the view that include members of a particular VLAN.

The submanagers are described in the following sections.

- [VLAN Manager](#) on page 79
- [MultiLink Trunking Manager](#) on page 80
- [Security Manager](#) on page 80
- [Routing Manager](#) on page 81
- [Trap/Log Manager](#) on page 81
- [Virtual Routing Manager](#) on page 82
- [Multicast Manager](#) on page 82
- [Bulk Configuration Manager](#) on page 83
- [VSN Manager](#) on page 83
- [Multimedia Manager](#) on page 84
- [Trap Viewer](#) on page 84
- [Syslog Viewer](#) on page 85

VLAN Manager

VLAN Manager enables you to manage VLAN and STG configurations across a single device or multiple devices. You can access the VLAN Manager only if the administrator has assigned this MEM role to you. In the VLAN Manager, you can only access the devices that are assigned to you by a security administrator.

With VLAN Manager you can perform the following tasks.

- add, delete, modify and monitor VLAN and Spanning Tree across one or more devices.
- view and edit VLAN nodes across the network.

- view and edit port membership information for ports not belonging to an STG.
- view and edit port membership information for ports belonging to one, or more than one STG.
- view and edit port membership information for individual routing ports and bridge routing ports.
- view Spanning Tree configuration information in the Configuration and Orchestration Manager (COM) topology map, such as the ports that are blocking or forwarding; the user device is the root of the Spanning Tree configuration.

For more information about the configuration of VLAN Manager, see *Avaya Configuration and Orchestration Manager Administration* (NN47226-600).

MultiLink Trunking Manager

MultiLink Trunking is a point-to-point connection that aggregates multiple ports so that they logically act like a single port with the aggregated bandwidth. Grouping multiple ports into one logical link means achieving higher aggregate throughput on a switch-to-switch or server-to-server application.

With Configuration and Orchestration Manager (COM) you can configure MultiLink Trunking across multiple devices, and perform the following tasks.

- Create, delete, or modify MultiLink Trunks (MLT) and Split Multilink Trunks (SMLT).
- View or configure MLT configuration information such as port and VLAN membership.

For more information about the configuration of MultiLink Trunking Manager, see *Avaya Configuration and Orchestration Manager Administration* (NN47226-600).

Security Manager

With Security Manager you can manage access to device and network management functions on network devices discovered by Configuration and Orchestration Manager (COM).

You can synchronize, change, and view security features for the following:

- Command Line Interface (CLI) access
- Web access
- Simple Network Management Protocol (SNMP) access
- Access policies
- Remote Access Dial-In User Services (RADIUS) properties

- SNMPv3 properties
- Secure Shell (SSH) bulk password
- Terminal Access Controller Access-Control System (TACACS)

You can configure the network access for each application using one or more security groups that you manage independently. If you want a group of devices to have the same passwords and access features, use security groups to group the devices together.

For more information about the configuration of Security Manager, see *Avaya Configuration and Orchestration Manager Administration* (NN47226-600).

Routing Manager

With Routing Manager you can configure routing parameters for devices across a network.

Routing Manager supports the following protocols.

- IP Routing
- RIP
- OSPF
- ARP
- VRRP
- IPv6 Routing
- IPv6 OSPF

Use Routing Manager to perform the following tasks.

- Create, delete, or modify routes across multiple devices.
- View and configure routes and properties for IP, RIP, OSPF, VRRP, IPv6, and IPv6 OSPF.

For more information about the configuration of Routing Manager, see *Avaya Configuration and Orchestration Manager Administration* (NN47226-600).

Trap/Log Manager

The Trap/Log Manager is a Configuration and Orchestration Manager (COM) submanager with which you can configure and view the traps or notifications, and the System Log. The Trap/Log Manager combines the functionality of the Trap Receiver and Log Manager

submanagers from previous releases, and provides additional capabilities to configure traps, notifications, and syslogs.

For more information about the configuration of Trap/Log Manager, see *Avaya Configuration and Orchestration Manager Administration* (NN47226-600).

Virtual Routing Manager

With Virtual Routing Manager you can manage configurations across specific devices. Additionally, you can set the current configuration for each device.

To start Virtual Routing Manager, the administrator must perform the following tasks:

- assign the VRM to you in the MultiElementManager Assignment tab.
- assign devices to you.

With Virtual Routing Manager you can perform the following tasks:

- view all VRFs and VRF statistics configured for a specific device.
- edit single or multiple VRF configurations.
- add a new VRF to a device.
- delete a VRF from a device.
- set the current VRF configuration for each device.

For more information about the configuration of Virtual Routing Manager, see *Avaya Configuration and Orchestration Manager Administration* (NN47226-600).

Multicast Manager

With the Avaya Configuration and Orchestration Manager (COM) Multicast Manager you can manage Avaya devices that support multicast. The Multicast manager displays multicast configurations across a network of devices. You can edit the Multicast Manager and highlight multicast information on the topology map; however, to fully configure the multicast network, you must use EDM or JDM.

The Multicast Manager displays the following multicast protocols supported on the devices discovered in the network topology:

- IGMP and IGMP Snoop
- DVMRP
- PIM-SM

- MSDP
- Multicast Route
- Policy

For more information about the Multicast Manager, see *Avaya Configuration and Orchestration Manager Administration* (NN47226–600).

Bulk Configuration Manager

You can launch the Bulk Configuration Manager (BCM) from the Configuration and Orchestration Manager (COM) Managers panel to create tasks and import devices.

The BCM has the following tools that can be instantiated more than one time in more than one tab:

- Configuration Backup and Restore
- Configuration Update Generator
- Device Password Manager
- Inventory
- Log browser
- License
- Scheduler
- Software version Updater
- Tunnel Guard Distributer

For more information about Bulk Configuration Manager, see *Avaya Bulk Configuration Manager Fundamentals* (NN48014–100).

VSN Manager

The Virtual Services Network (VSN) Manager is a multielement manager with which you can manage L2 Shortest Path Bridging MAC (SPBm) and L3 SPBms throughout the discovered network on ERS 8600 version 7.1 devices, and VSP 9000 devices. The VSN Manager provides a device-centric view of the VSNs, and a VSN-centric view of the networks.

With the VSN Manager you can perform the following tasks:

- configure and view L2 SPBms and L3 SPBms throughout the discovered network on ERS 8600 version 7.1 devices
- add, delete, or edit L2 SPBms and L3 SPBms across multiple devices

For more information about the VSN Manager, see *Avaya Configuration and Orchestration Manager Administration* (NN47226–600).

Multimedia Manager

The Avaya Configuration and Orchestration Manager (Avaya COM) Multimedia Manager manages Auto Detection/Auto Configuration (ADAC) and 802.1ab parameters of the Avaya switch. With ADAC, a switch supports and prioritizes Avaya IP Phone traffic without administrator intervention. With ADAC enabled, the switch automatically detects an Avaya IP phone after the phone connects to the switch, and then automatically configures the VLAN, port, and QoS settings for the phone.

Multimedia Manager supports the following 802.1ab parameters.

- For LLDP—Globals, Ports, and Neighbor
- For Port dot1—Local VLAN Id, Local Protocol VLAN, and Local VLAN Name
- For Port dot3—Local PoE, Local Link Aggregate, and Local Max Frame
- For Port med—Local Policy, Local Location, Local PoE PSE, Neighbor Capabilities, and Neighbor Inventory

For more information about Multimedia Manager, see *Avaya Configuration and Orchestration Manager Administration* (NN47226–600).

Trap Viewer

The Trap Viewer is a Configuration and Orchestration Manager (COM) tool with which you can view traps and notifications for devices. You can export information from the Trap Viewer to a text file; however, you cannot edit cells.

Trap parser configuration

You can use the **Trap Viewer** tab to configure trap parsers and to assign colors to trapped OID values in the COM database. The color that you assign to an OID value represent its importance in the trap grid listings. You can visually manage the network by setting severities for network events or statuses according to OID values.

For example, you can specify that a trap containing a specific OID should be considered a high priority trap and should be highlighted in red. When configured correctly, the COM application displays the trapped OID value in red in the trap grid.

For more information about the Trap Viewer and trap parser configuration, see *Avaya Configuration and Orchestration Manager Administration* (NN47226–600).

Syslog Viewer

The Syslog Viewer is a Configuration Orchestration Manager (COM) tool with which you can view the system log. You can export information from the Syslog Viewer to a text file; however, you cannot edit cells.

For more information about the Syslog Viewer, see *Avaya Configuration and Orchestration Manager Administration* (NN47226–600).

Chapter 11: Wizards and templates overview

Avaya Configuration and Orchestration Manager (COM) wizards help you to configure complex network topologies and deployments using minimal procedure steps.

The template in COM contains a set of configuration attributes. You can create templates by operating COM configuration wizards. At any point while running the wizard, you can save the wizard configurations as a template. You can view the saved templates in the Templates dialog box, and use the templates to easily perform the same or similar configurations that the wizards perform.

Wizards management

There are three types of wizards:

- **VLAN Wizard**—Use to configure STG and VLAN in multiple devices.

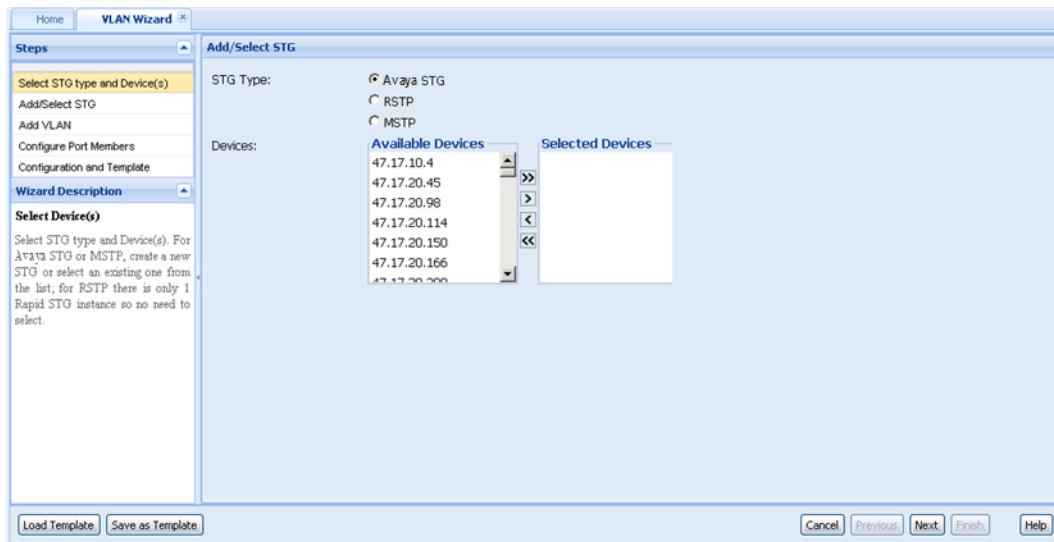


Figure 5: VLAN Wizard

- **SMLT Wizard**—Use to create trunks configurations including necessary VLAN creation, various protocol enabling, and miscellaneous device settings.

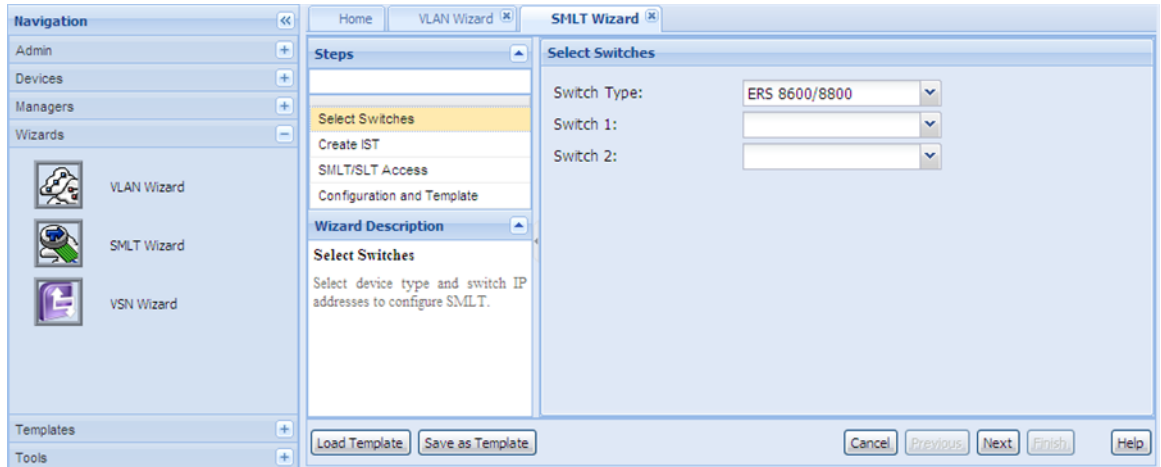


Figure 6: SMLT Wizard

- **VSN Wizard**—Use to configure VSN service on multiple devices. The VSN Wizard is composed of the following wizards:
 - SPB Infrastructure Wizard
 - L2 SPB Service Wizard
 - L3 SPB Service Wizard

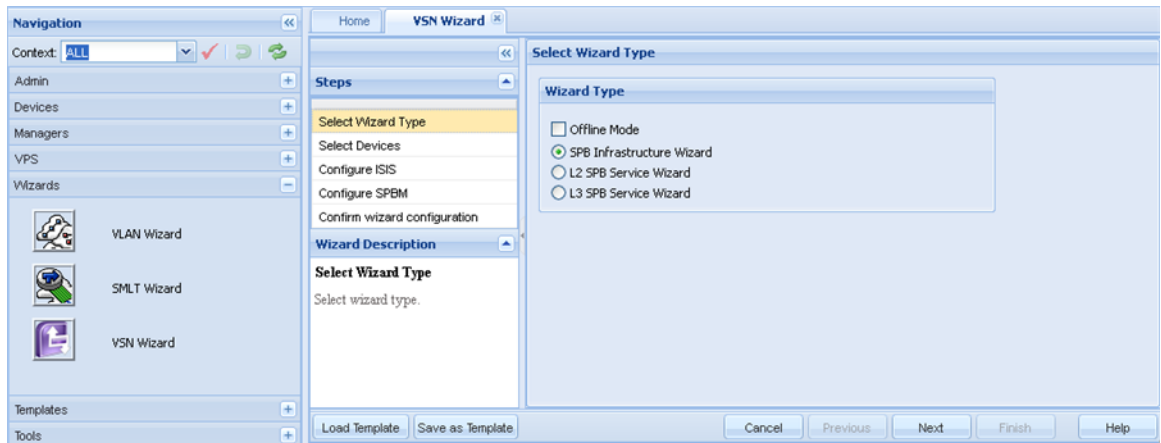


Figure 7: VSN Wizard

To select a wizard, from the COM navigation pane, select Wizards, and then click VLAN Wizard, SMLT Wizard, or VSN Wizard.

The following figure shows the Wizards panel in the Navigation pane.

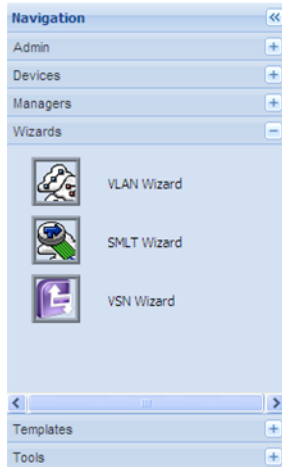


Figure 8: Wizards panel

For more information about the configuration of VLAN wizard, SMLT wizard and VSN wizard, see *Avaya Configuration and Orchestration Manager Administration* (NN47226-600).

Templates management

There are three types of templates:

- **VLAN**—The VLAN template consists of one STG and multiple VLANs. You can select a VLAN template, and load it in to VLAN configuration wizard. In VLAN wizard, you can change the configurations which are loaded from the VLAN template, or add additional configurations for device specific attributes.
- **SMLT**—The SMLT template consists of SMLT/SLT and VLAN configuration. You can select a SMLT template, and load it in to SMLT configuration wizard. In SMLT wizard, you can change the configurations which are loaded from the SMLT template, or add additional configurations for device specific attributes
- **VSN**—You can save VSN wizard templates as L2 SPB service, L3 SPB service, and SPB infrastructure. Configuration and Orchestration Manager (COM) loads the data you save in a template file into each wizard type, and then programs the data on the device through a telnet connection. Because COM discovers data, and data may or may not exist on the device, some template data is not used. You can select a VSN template, and load it in to the VSN configuration wizard. In the VSN wizard, you can change the configurations which are loaded from the VSN template, or add additional configurations for device specific attributes.

To view the Templates dialog box, from the COM Navigation pane, select Templates, and then click Templates.

The following figure shows the templates dialog box.

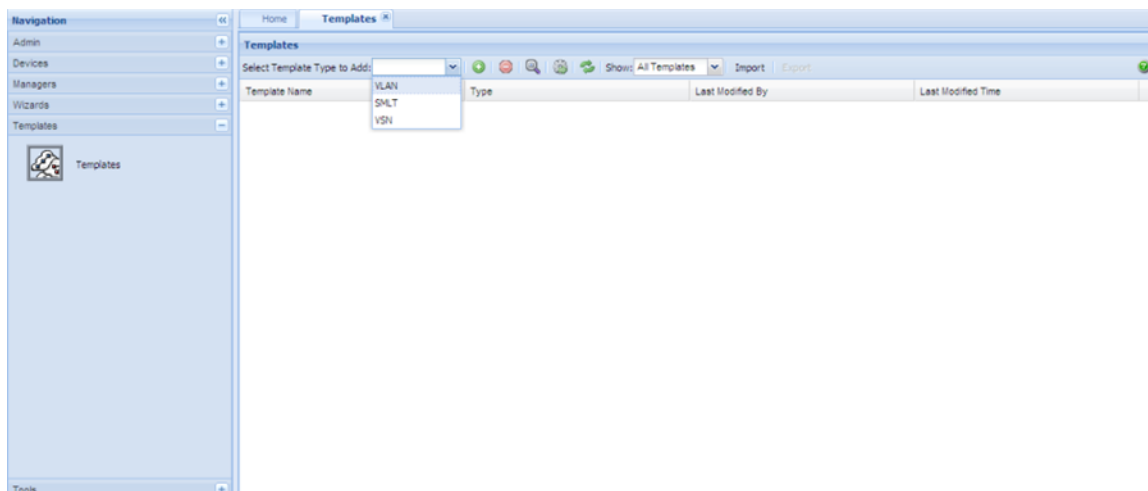


Figure 9: Templates dialog box

For more information about configuring templates, see *Avaya Configuration and Orchestration Manager Administration* (NN47226-600).

Chapter 12: Maintenance

This chapter provides information about the tools supported by Avaya Configuration and Orchestration Manager (COM), including the SmartDiff Tool, TFTP Server, MIB Browser, Port Scanner, and Scheduled Tasks tools. Configuration and Orchestration Manager also provides a CLI manager and a Configuration Auditing Tool.

Navigation

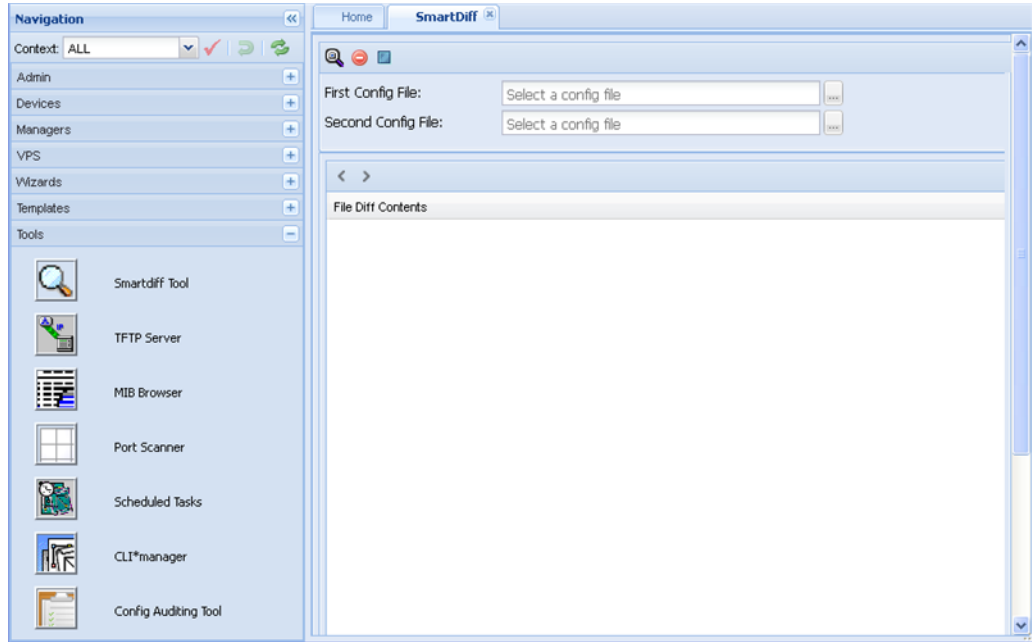
- [Starting the SmartDiff Tool](#) on page 91
- [Viewing the TFTP Server](#) on page 93
- [MIB Browser](#) on page 97
- [Accessing the Port Scanner](#) on page 104
- [Managing Scheduled Tasks](#) on page 108
- [Launching CLI*manager](#) on page 110
- [Launching the Configuration Auditing Tool](#) on page 117

Starting the SmartDiff Tool

With the SmartDiff tool you can compare two configuration files that have a .cfg extension. Perform the following procedure to start the SmartDiff tool.

Procedure steps

1. In the Navigation pane, select the **Tools** panel.
2. Click the **SmartDiff Tool** icon.



The following figure shows the SmartDiff toolbar.



Figure 10: SmartDiff toolbar

Comparing configuration files

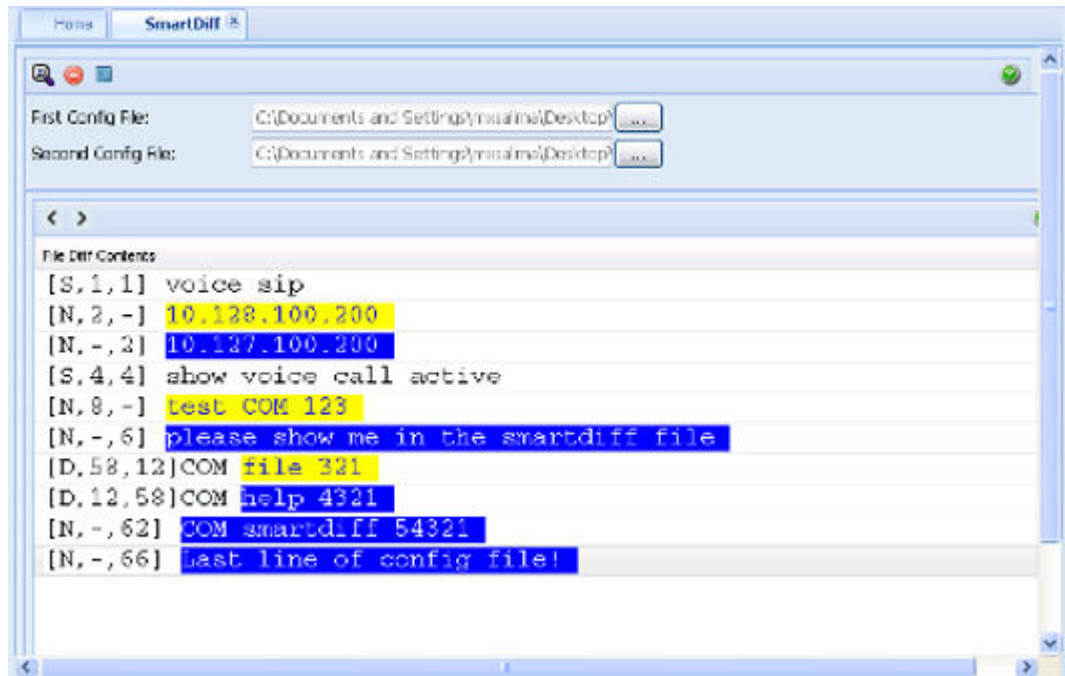
Perform the following procedure to compare two configuration files.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **SmartDiff Tool**.
2. In **First Config File** and **Second Config File** fields, enter the name of the configuration files you want to compare. Use the ... buttons to browse the files.

To reset the values in the **First Config File** and **Second Config File** fields, click **Reset the input controls**.

3. From the toolbar, click **Show differences between files**. The File Diff Contents panel contains the output of compare operation as shown in the following figure.



The Status bar displays the comparison report including whether the files are identical or different, and the number of different lines. SmartDiff Tool highlights the content in three colors—white, blue, and yellow. The significance of these colors are as follows:

- Black text in a white background indicates the matched text in a line.
- Blue Text in a yellow background indicates any different text in the first line.
- White text in a blue background indicates any different text in the second line
- Black text in a grey background indicates the modified lines in the file.

To navigate from one modified section to the next, use the arrows in the toolbar.

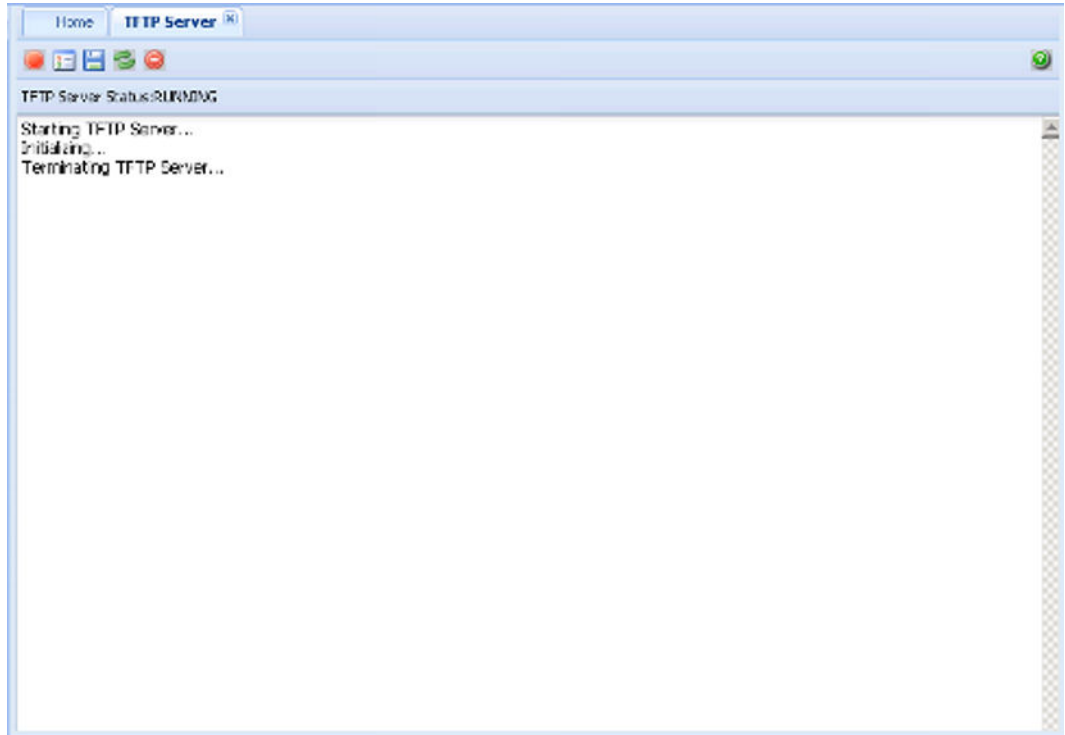
Viewing the TFTP Server

With the TFTP Server tool, you can view the status of the TFTP server, start or stop the TFTP server, and manage logs.

Perform the following procedure to view the TFTP server.

Procedure steps

1. In the Navigation pane, select the **Tools** panel.
2. Click **TFTP Server**.



The following figure shows the TFTP Server toolbar.



Figure 11: TFTP Server toolbar

Navigation

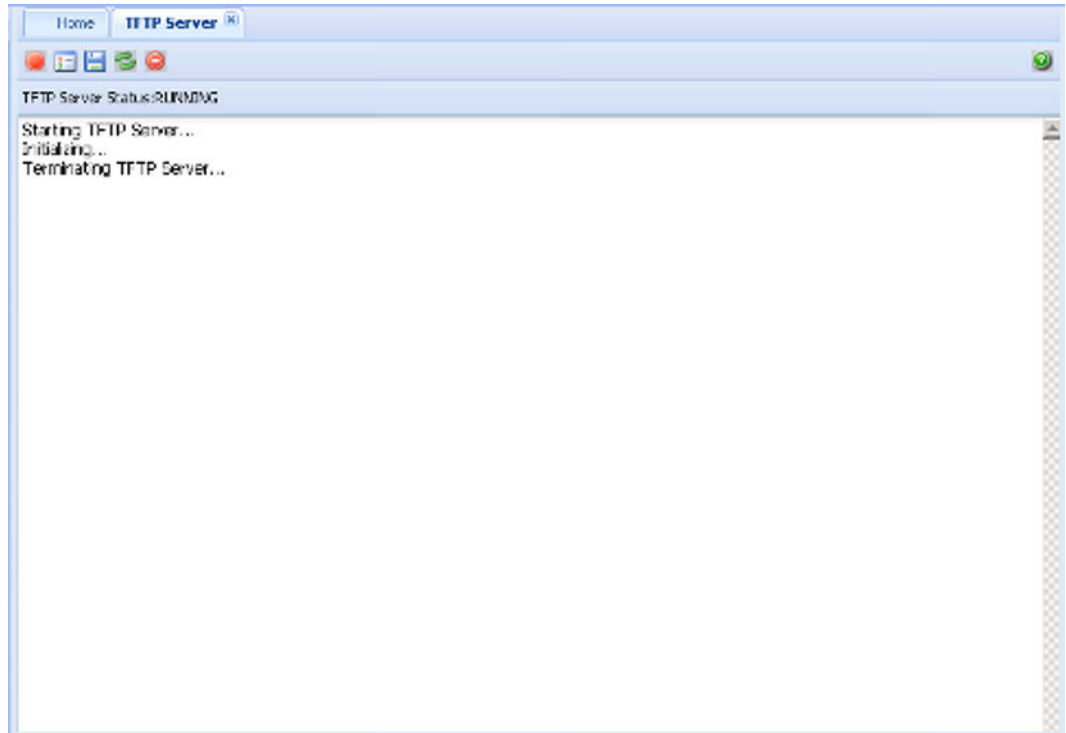
- [Viewing the TFTP Server status](#) on page 95
- [Starting and stopping the TFTP Server](#) on page 95
- [Editing preferences](#) on page 96
- [Saving log messages](#) on page 97
- [Refreshing log messages](#) on page 97
- [Clearing log messages](#) on page 97

Viewing the TFTP Server status

Perform the following procedure to view the status of the TFTP server.

Procedure steps

1. In the Navigation pane, select the **Tools** panel.
2. Click **TFTP Server**.



Starting and stopping the TFTP Server

Perform the following procedure to start or stop a TFTP server.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **TFTP Server**.
2. If the TFTP Server Status is running and you want to stop the TFTP Server, then from the toolbar, click **Stop TFTP Server**. After stopping the TFTP Server, this button turns to **Start TFTP Server**.

If the TFTP Server Status is already stopped and you want to start the TFTP Server, then from the toolbar, click **Start TFTP Server**. After you start the TFTP Server, this button turns to **Stop TFTP Server**.

Editing preferences

Perform the following procedure to edit TFTP Server preferences.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **TFTP Server**.
2. From the toolbar, click **Preferences**.

3. Update the field you want to modify, and then click **OK** to commit the changes, or click **Cancel** to discard the changes.

Job aid

The following table describes the fields of the TFTP Server Preference dialog box.

Table 15: TFTP Server Preferences table

Tab	Description
Root Directory	Specifies the root directory in the TFTP Server.
Log File Name	Specifies the log file name.
SocketTimeout (1–30 secs)	Specifies the socket timeout for the log files created. The default value is 8.
Max Retries (0–5)	Specifies the maximum retries for the log files. The default value is 3.
Trace Mode	Specifies the Trace Mode.

Saving log messages

Perform the following procedure to save the current TFTP server log.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **TFTP Server**.
2. From the toolbar, click **Save Log Messages** to save the current TFTP server log.

Refreshing log messages

Perform the following procedure to refresh the current TFTP server log.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **TFTP Server**.
2. From the toolbar, click **Refresh Log** to refresh the current TFTP server log.

Clearing log messages

Perform the following procedure to clear the TFTP server log.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **TFTP Server**.
2. From the toolbar, click **Clear Log Messages**. After you are prompted to confirm the clearing of log messages, click **Yes** to clear the current TFTP server log.

MIB Browser

With the MIB Browser you can manage SNMP-enabled network devices and applications. You can load, browse, and search MIBs, walk the MIB tree, and perform all other SNMP-related functions using the MIB Browser. You can also view and operate the data available through an SNMP agent in a managed device.

The following figure shows the MIB Browser tab.

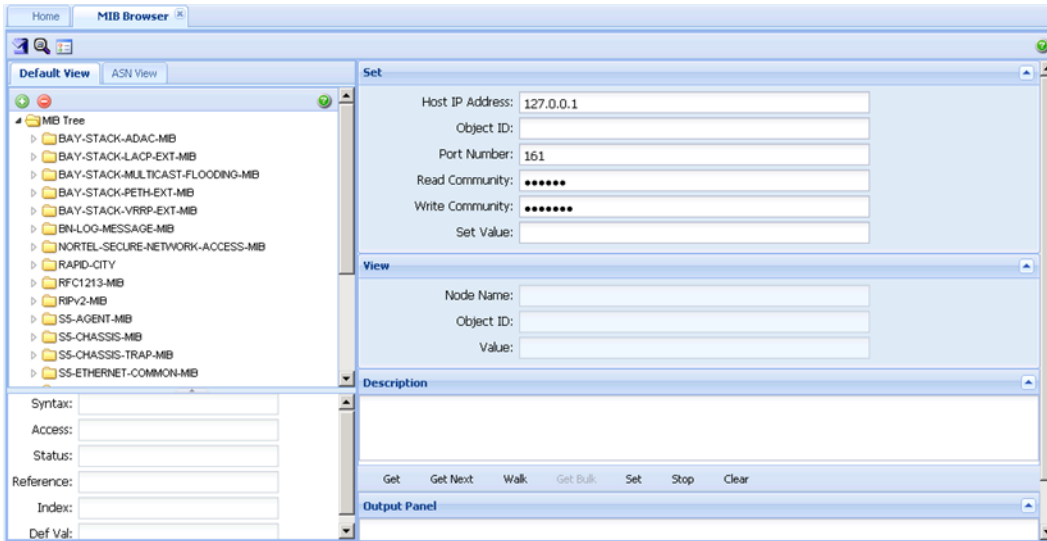


Figure 12: MIB Browser




The following table describes the parts of the MIB Browser tab.




Table 16: Parts of the MIB Browser tab

Part	Description
Views	Displays the currently loaded MIBs. The available views are: Default view, and ASN view. The ASN view shows all MIBs in ASN format.
Set panel	Use to set the host IP to which you want to communicate .
View panel	Displays the details of the selected MIB name.
Description panel	Displays the description of the selected MIB.
Menubar	Provides quick access to commonly used SNMP commands.
Output Panel	Displays output of the operation performed using menubar options.

The following table describes the tools available for the MIB Browser tab.

Table 17: MIB Browser tools

Tool	Icon	Description
Load MIB		Use to load an MIB.
Unload MIB		Use to unload an MIB.
Set SNMP Version		Use to set the SNMP version. The available versions are as follows:

Tool	Icon	Description
		<ul style="list-style-type: none"> • SNMP v1 • SNMP v2c • SNMP v3
SNMP Bulk Settings		Opens Get Bulk Panel.
SNMPV3 Settings		Opens SNMPV3 Panel.
Help		Opens Online Help.

Navigation

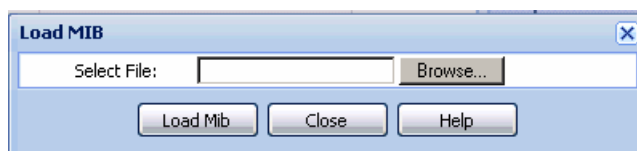
- [Loading an MIB](#) on page 99
- [Unloading an MIB](#) on page 100
- [Setting SNMP version](#) on page 100
- [Retrieving data of an MIB node](#) on page 101
- [Traversing the MIB tree](#) on page 101
- [Retrieving the value of a subtree](#) on page 102
- [Retrieving data from a large table](#) on page 102
- [Editing data for an MIB node](#) on page 103

Loading an MIB

Perform the following procedure to load an MIB.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **MIB Browser**.
2. Click the **Default View** or **ASN View** tab.
3. From the toolbar, click the **Load MIB** icon (+).



4. In Select File field, enter the MIB file you want to load. Use Browse to select the MIB file.
5. Click **Load MIB** to load the selected MIB.

The loaded MIB appears at the end of the MIB tree in Default View.

You can click **Close** to cancel the loading.

Unloading an MIB

Perform the following procedure to unload an MIB.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **MIB Browser**.
2. Click the **Default view** tab, and select the MIB node you want to delete.
3. From the toolbar, click the **Unload MIB**.
4. Click **Yes** to unload the selected MIB.

To cancel the unload operation, click **No**.

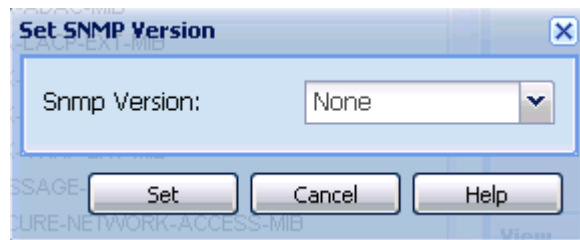
If you click Yes, the MIBs are removed from the tree.

Setting SNMP version

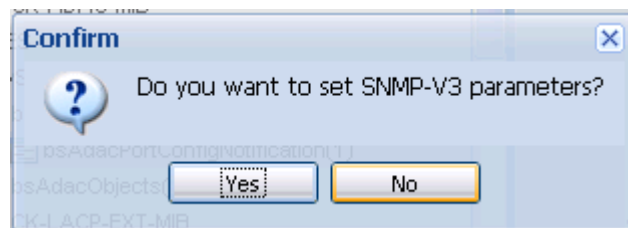
Perform the following procedure to set SNMP version of a MIB.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **MIB Browser**.
2. Click the **Default view** or **ASN View** tab, and then select an MIB which SNMP you want to change.
3. From the toolbar, click **Set SNMP Version**.



4. Choose the version that you want to set in the **Snmp Version** field.
5. Click **Set**.



- In the Confirm dialog box, click **Yes**.



The image shows a dialog box titled "SNMP-V3 Settings" with a close button (X) in the top right corner. Inside the dialog, there is a section titled "SNMP-V3 Parameters" containing five fields: "User Name:" (text input), "Authentication:" (dropdown menu with "None" selected), "Auth. Password:" (text input), "Privacy:" (dropdown menu with "None" selected), and "Privacy Password:" (text input). At the bottom of the dialog, there are two buttons: "Ok" and "Close".

- Complete the fields in the SNMP-v3 Settings dialog box as appropriate, and then click **Ok**.

In the Set Panel, the **Read Community** and **Write Community** parameters of SNMP V1 and SNMP V2C are replaced by the SNMP-v3 parameters **Context Name** and **Context Engine**. The Set Panel is updated with the new settings.

- Enter the value of fields in **Set** panel as appropriate.

Retrieving data of an MIB node

Perform the following procedure to retrieve the value of the leaf object from the managed objects.

Procedure steps

- In the Navigation pane, select the **Tools** panel, and then click **MIB Browser**.
- Select a node from the MIB tree.
- Click **Get** from the menubar.

Traversing the MIB tree

Perform the following procedure to retrieve the value of the next OID in the MIB tree.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **MIB Browser**.
2. Select a node from the MIB tree.
3. Click **Get Next** from the menubar.

Retrieving the value of a subtree

Perform the following procedure to retrieve the value of all child nodes of the MIB node you select.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **MIB Browser**.
2. Select a node from the MIB tree.
3. Click **Walk** from the menubar.

Retrieving data from a large table

Perform the following procedure to retrieve data from a large table.

Important:

The GetBulk operation is applicable only on SNMPv2c and SNMPv3.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **MIB Browser**.
2. Select a node from the MIB tree.
3. Ensure that the SNMP version is set to either SNMPv2c or SNMPv3. For more information on changing SNMP version, see [Setting SNMP version](#) on page 100.
4. From the toolbar, click **SNMP Bulk Setting**.
5. Select a node from the MIB that you want to add to the variable-bindings list, and then click **Add**.
6. Enter the value in the **Max. Repetitions** and **Non Repeaters** fields.
7. Click **Get Bulk** from the menubar to the bulk SNMP data.

The MIB Browser retrieves the sequence of next objects immediately after the specified object. The number of object instances returned is equal to the Max-Repetitions field.

Editing data for an MIB node

Perform the following procedure to modify the data for one or more MIB variables.

! Important:

You can perform the Set operation only on a node that has read-write access.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **MIB Browser**.
2. Select a node from the MIB tree.
3. From the Set panel, enter the value you want to configure in the Set Value field.
4. From the menu bar, click **Set**.

Job aid

The following table describes the fields of the Get Bulk Panel.

Table 18: Get Bulk Panel

Field	Description
Max. Repetitions	Specifies the number of lexicographic successors to be returned for the remaining variables in the variable-bindings list.
Non Repeaters	Specifies the number of variables in the variable-bindings list for which a single lexicographic successor is to be returned.
Add	Adds the selected MIB variable to the variable-bindings list.
Delete	Removes the selected node from the variable-bindings list.
Done	Closes the GetBulk Settings pane.

Job aid

The following table describes the fields of the SNMP-V3 Settings dialog box.

Table 19: SNMP-V3 Settings dialog box

Field	Description
User Name	Specifies the SNMPv3 user name.
Authentication	Specifies the Authentication protocol used.

Field	Description
Auth Password	Specifies the password that is used for authentication purposes.
Privacy	Specifies the privacy protocol used.
Privacy Password	Specifies the password that is used for privacy purposes.

Accessing the Port Scanner

With the Port Scanner you can scan the target devices. Port Scanner enables parameters to configure periodic port scan, and store exported port scan data into files. Perform the following procedure to view the Port scanner dialog box.

Procedure steps

1. In the Navigation pane, select the **Tools** panel.
2. Click **Port Scanner**.



Navigation

- [Scanning Ports](#) on page 105
- [Exporting a report of port scan](#) on page 105
- [Scheduling a scan](#) on page 105
- [Viewing scan results](#) on page 106

Scanning Ports

Perform the following procedure to scan ports of the selected device.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **Port Scanner**.
2. In the **Available Device** field, select the devices you want to scan and use **>** or **>>** to move the devices to **Selected Devices** field.
3. From the toolbar, click **Scan Ports**.

The result appears in the content pane, in both the Port Scan tab and the Port Status tab.

Exporting a report of port scan

Perform this procedure to export the report of port-scan.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **Port Scanner**.
2. In the **Available Device** field, select the devices you want to scan, and use **>** or **>>** to move the devices to the **Selected Devices** field .
3. From the toolbar, click the **Scan Ports**.
4. To export the report, from the toolbar, click **Export**.
5. Select **Text** or **Html**.
6. Select **port scan** or **port status**, or both **port scan** and **port status**.
7. Click **Ok**.

Scheduling a scan

Perform the following procedure to schedule a scan of a device or devices.

Procedure

1. From the Navigation pane, open the **Tools** panel, and then click **Port Scanner**.
2. In the Available Devices field, select the devices you want to scan, and click the right-pointing arrow.
 - To select all devices, click the double right-pointing arrow.

- To remove a device from the Selected Device list, select the device and click the left-pointing arrow.
 - To remove all devices from the Selected Device list, click the double left-pointing arrow.
3. Click **Schedule Scan**.
 4. Enter the Task Name.
 5. Enter the Schedule Name.
 6. Select a scheduled time frame of the scan.
 7. Select the date and time of the scan.
If you select a schedule that does not require a date entry, the date field is unavailable.
 8. Click **Set**.
-

Viewing scan results

Perform the following procedure to view scan results.

Before you begin

- You must schedule a scan before you can view the scan results.

Procedure

1. From the Navigation panel, open the **Tools** panel, and then click **Port Scanner**.
2. In the Available Devices field, select the devices you want to scan, and click the right-pointing arrow.
 - To select all devices, click the double right-pointing arrow.
 - To remove a device from the Selected Device list, select the device and click the left-pointing arrow.
 - To remove all devices from the Selected Device list, click the double left-pointing arrow.
3. From the Port Scanner tool bar, click **Schedule Scan**.
4. Enter the Task Name.
5. Enter the Schedule Name.
6. Select a scheduled time frame of the scan.
7. Select the date and time of the scan.

If you select a schedule that does not require a date entry, the date field is unavailable.

8. Click **Set**.
9. From the Port Scanner tool bar, click **View Scan Results**.
10. To close the window, click **Ok**.

Job aid

The following table describes the parts of Port Scanner tab.

Table 20: Port Scan tab

Part	Description
Toolbar	Provides you with the following Port Scanner tools: <ul style="list-style-type: none"> • Scan Ports—scans the target devices. • Export—exports the result in text format. • Schedule Scan—schedules a scan. • View Scan Results—displays results of a port scan.
Available Devices	Contains a list of assigned devices.
Selected Devices	Contains devices selected from the Available Devices list.
>>	Use to move all the devices from the Available Devices list into the Selected Devices list.
>	Use to move the selected device from the Available Devices list into the Selected Devices list.
<	Use to move the selected device from the Selected Devices list to the Available Devices list.
<<	Use to move all the devices in the Selected Devices list to the Available Devices list.
Host IP	Specifies the IP addresses of the target devices.
Port	Specifies the device ports.
Available MACs	Specifies the MAC addresses of device ports.
Target Devices	Specifies the IP address if the available MAC.

Job aid

The following table describes the parts of the Port Status tab.

Table 21: Port Status tab

Part	Description
Host IP	Specifies the IP addresses of the target devices.
Port	Specifies the device ports.
Port Status	Specifies the status of the port.
Last Change	Specifies when the last port status change occurred.

Managing Scheduled Tasks

With the Scheduled Tasks tool, you can view, delete, cancel or reschedule tasks from the Inventory Manager. Perform the following procedure to view the scheduled tasks.

Procedure steps

1. In the Navigation pane, select the **Tools** panel.
2. Click **Scheduled Tasks**.

The following table describes the tools of Scheduled Tasks tab.

Table 22: Scheduled Tasks tools

Tool	Description
Refresh	Refreshes the scheduled task list.
Delete Task	Deletes the selected scheduled task.
Cancel Task	Cancels the selected scheduled task.
Reschedule Task	Reschedules the selected scheduled task.
Run Task	Immediately runs the selected scheduled task.

Navigation

- [Refreshing the scheduled task list](#) on page 109
- [Deleting a scheduled task](#) on page 109
- [Canceling a scheduled task](#) on page 109
- [Rescheduling a scheduled task](#) on page 110
- [Running a scheduled task](#) on page 110

Refreshing the scheduled task list

Perform the following procedure to refresh the scheduled task list.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **Scheduled Tasks**.
2. Click **Refresh**.

Deleting a scheduled task

Perform the following procedure to delete a scheduled task.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **Scheduled Tasks**.
2. Select the task that you want to delete, and then click **Delete Task**.

Canceling a scheduled task

Perform the following procedure to cancel a scheduled task.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **Scheduled Tasks**.
2. Select the task that you want to cancel, and then click **Cancel Task**.

Rescheduling a scheduled task

Perform the following procedure to reschedule a scheduled task.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **Scheduled Tasks**.
2. Select the task that you want to reschedule, and then click **Reschedule Task**.

Running a scheduled task

Perform the following procedure to run a scheduled task.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **Scheduled Tasks**.
2. Select the task that you want to run, and then click **Run Task**.

Launching CLI*manager

CLI*manager speeds up and simplifies operations and provisioning for a large number of Avaya device types. CLI*manager offers a set of basic features for all device type, and enhanced features for specific device types. The basic feature set includes simultaneous control of multiple devices, proxy connections, WATCH monitoring, automation, scripting, tabbed sessions, and logging.

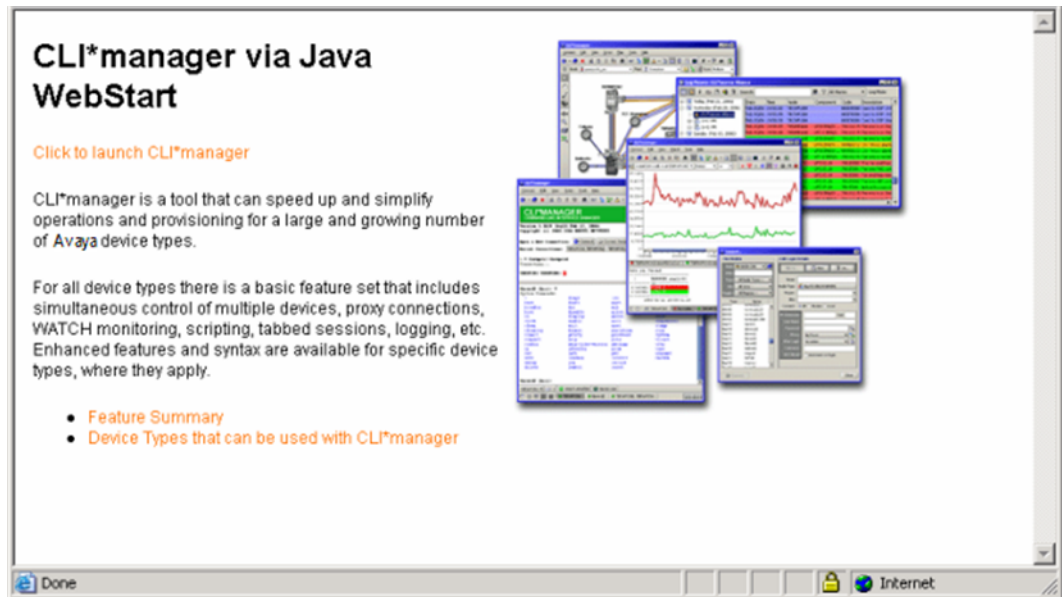
Prerequisites

- You must install Java Virtual Machine (JVM).

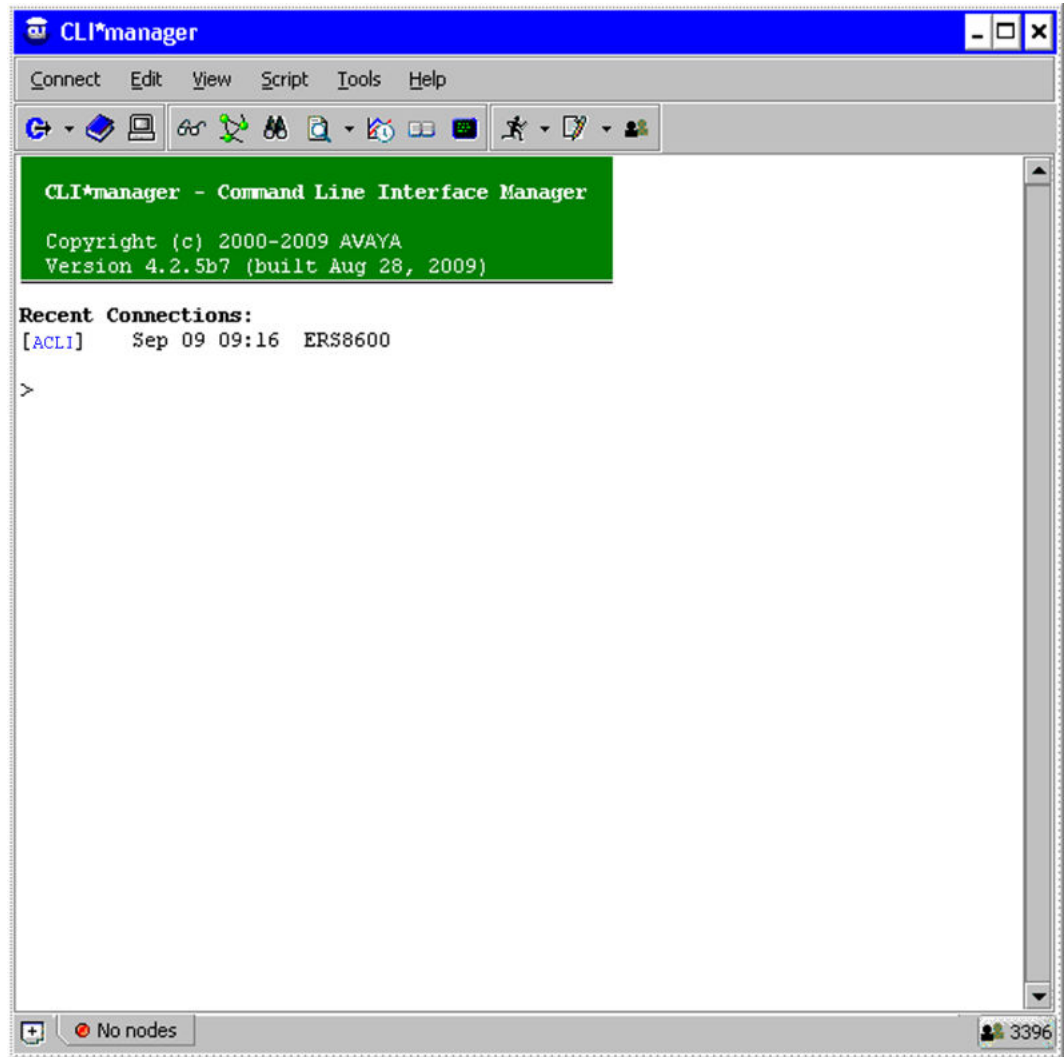
Perform the following procedure to launch the CLI*manager.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **CLI*manager**.



2. Click the **Click to launch CLI*manager** link.
3. In the Warning — Security dialog box, click **Yes**.



Navigation

- [CLI*manager user interface](#) on page 113
- [Connection set up](#) on page 113
- [Supported device type](#) on page 114

CLI*manager user interface

The CLI*manager user interface has the following features:

- Main toolbar—Provides quick access to commonly-used features.
- Options window—Enables the change of many properties of the CLI*manager interface.
- Session tabs—Represent active CLI sessions. Each tab shows the names of the active devices in a session, along with a small icon showing the current status of the session. With session tabs, you can quickly switch between multiple active CLI sessions.
- User buttons—An optional toolbar that appears at the bottom of the main CLI*manager window.
- Node tree—Displays a graphical tree for components in the connected MSS, and shows trees based on saved ASCII provisioning files.
- Flowcharts—Help you to draw flowcharts that integrate with the command-line. Buttons on the flowchart symbols can run commands and scripts, and can link to other flowcharts.
- FTP/SFTP window—Transfers files to and from remote devices. You can specify the remote device using either an address book entry, or manually by providing an address, user name, and password.
- File Server profiles—Used by a number of features in CLI*manager including Shared Address Books and autouploading Log Files.
- File synchronization—Copies sets of CLI*manager files from remote file server directories into local CLI*manager directories, and checks for updates either periodically or on demand.
- Table viewer—Displays tables from MSS commands and TL1 commands on optical nodes in a graphical, spreadsheet format.
- Command history—Recalls previous commands. Use the standard up-and-down arrow keys to open a pop-up window for browsing to recent commands.
- Search—Finds specified text anywhere in the CLI window.

Connection set up

Login information is stored in encrypted Address Books that can be shared among groups of users and updated from within CLI*manager using centralized File Server Profiles. Connections are made using both IP (Telnet, SSH, and Rlogin) and Serial (local port or modem). Many different kinds of Proxies are used to set up connections through gateways, firewalls, and modem pools. File transfers are done using FTP, SFTP, and TFTP. SSH Tunnels can be used to tunnel through intermediate SSH devices. SSH X11 port forwarding allows X

applications to run through an encrypted SSH channel. Any number of users can collaborate by sharing sessions with each other and typing on the same command line.

Supported device type

CLI*manager is used with a large and growing number of device types. CLI*manager provides a set of basic features available for all types, and some enhanced features and syntax available for specific device types.

- Application Switches
 - Alteon Switch Firewall System
 - Alteon Web Switch 184/AD3/AD4
- Ethernet Switches / Routers
 - BayStack 450/460/470
 - Business Policy Switch (BPS)
 - Centillion
 - Ethernet Routing Switch 1200/1600/4500/5500/8100/8600/8800
 - Metro Ethernet Switching Unit 1800/1860
 - Avaya Secure Router 1000, 3120, 6230,6280
 - Virtual Services Platform (VSP) 9xxx
- MultiProtocol Routers
 - Access Remote Node (ARN)
 - Access Stack Node (ASN)
 - Backbone Concentrator Node (BCN)
 - Backbone Link Node (BLN)
- MultiService Switches / Edge
 - Avici
 - MPE 9000
 - Passport 4400 Multiservice Access
 - Passport 6400 Multiservice Edge
 - Passport Multiservice Switch 7400/15000/20000
 - Services Edge Router 5500
- Non-Avaya
 - Airvana DOM/RNC

- CVX
- IOS
- Juniper T/M/J Series
- Optical
 - Common Photonic Layer
 - EC1
 - HDX
 - Long Haul 1600
 - OC12
 - OC192
 - OC48
 - Operations Controller (OPC)
 - OPTera DX
 - Optical Metro 1000/3300/3400/3500/5000
 - Optical Multiservice Edge 1010/1030/1060/6500/6500BB
 - Optical Packet Edge (OPE)
 - Transport Node TN4X/TN16X/TN64X
- Other
 - Generic Secure Shell (SSH)
 - Generic Telnet
 - UNIX / Linux
 - VSE Platform
- Storage Networking
 - BCS3000 (Business Continuity System)
- Voice / Multimedia
 - Border Control Point 7100/7200
 - CICM
 - Communication Server 1000/1500/2000
 - DMS
 - IEMS
 - ITG
 - MCS 5100

- Media Gateway 9000
- Meridian-1
- MG9K Element Manager
- Neura BTX Media Gateway
- Neura NetConductor
- SAM21 Shelf Controller
- Session Server Lines/Trunks
- Signaling Server
- Spectrum Peripheral Module
- Succession GWC
- Succession Media Card
- USP
- XA-Core
- VPN Routers
 - Contivity 1000
- Wireless Networks
 - ASG 5000
 - BTS (Base Transceiver System)
 - DMS-MSC
 - DMS-MTX
 - GGSN (GPRS Support device)
 - GSM / UMTS Media Gateway R4/R5
 - InterWorking Function (IWF)
 - Media Gateway (CDMA)
 - PCUSN
 - PDSN – Shasta
 - PDSN 16000
 - RNC (Radio Network Controller)
 - SGSN (GPRS Support device)
 - ST CPE
 - Wireless AP 7220
 - Wireless AP 8120

- WLAN Access Point 2220/2221/2300
- WLAN Security Switch 2700
- Wireless Controller (WC) 8180

Launching the Configuration Auditing Tool

With the Configuration Auditing Tool you can retrieve configuration information from a device and compare it to reference data. You can retrieve the configuration information by entering the IP address of a device in the Configuration Auditing Tool. The Configuration Auditing Tool uses telnet credentials.

Use the following procedure to launch the Configuration Auditing Tool.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click **Config Auditing Tool**.
2. Click **Configuration Audit**.
3. Enter the IP address of the device you want to audit.
4. Click **Audit**.

A status dialog indicates that the audit is in progress. When the audit is complete, the tool displays information about the device configuration, as described in the table below.

5. To save the audit information in PDF format, click **Export** on the upper left of the panel, and then select **PDF**.

Table 23: Job aid

Item	Description
Issue	Specifies the configuration issue, and a recommendation for addressing the issue. For example, checksum settings, card status, and other settings are displayed.
Priority	Specifies the severity of the issue. For example, whether the issue identified is a warning, or a critical issue.
Device address	Specifies the IP address of the device audited.
Device type	Specifies the type of device audited.
Agent version	Specifies the agent version of the device audited.

Chapter 13: Supported devices

The following table lists the supported devices and device image versions.

Table 24: Device Requirements

Product family	Model	Versions
Belden L2E Switch	Hirschmann MICE-L2E	v.6.0.2
Belden L2P Switch	Hirschmann Railswitch –L2P	v.6.0.2
Belden L3P Switch	Hirschmann MACH-L3P	v.6.0.2
Avaya Ethernet Routing Switch	8600 series	v.4.0, v.4.1, v.5.0, v.5.1, v.7.0, v.7.1, and v.7.1.3
Ethernet Routing Switch	8800 series	v.4.0, v.4.1, v.5.0, v.5.1, v.7.0, v.7.1, and v.7.1.3
Ethernet Routing Switch	5510 series	v.5.1, v.6.0, v.6.1, v.6.2, and v.6.3
Ethernet Routing Switch	5520 series	v.5.1, v.6.0, v.6.1, v.6.2, and v.6.3
Ethernet Routing Switch	5530 series	v.5.1, v.6.0, v.6.1, v.6.2, and v.6.3
Ethernet Routing Switch	56xx series	v.5.1, v.6.0, v.6.1, v.6.2, and v.6.3
Ethernet Routing Switch	45xx series	v.5.2, v.5.3, v.5.4, v.5.5, v.5.6, 5.6.1 (limited), and 5.6.2 (limited)
Ethernet Routing Switch	48xx	v.5v.5.2, v.5.3, v.5.4, v.5.5, v.5.6, 5.6.1 (limited), and 5.6.2 (limited).2, v.5.3, v.5.4, v.5.5, and 5.6
Ethernet Routing Switch	3500	v.5.0
Ethernet Routing Switch	25xx series	v.4.1.x , v.4.2, v.4.3, and v.4.4
Ethernet Routing Switch	16xx series	v.2.1.5.x and v.2.1.6.x
Virtual Services Platform	7024	v.10.1 and 10.2
Virtual Services Platform	9000 series	v.3.0, v. 3.1, v.3.2, and v.3.3
Wireless Controller	8180	v.1.0, v.1.1, and v.1.2

Supported devices

Product family	Model	Versions
Wireless LAN AP	23xx. AP 23xx	v.1.3
Wireless LAN AP	8120	v.1.0, v.1.1, and v.1.2
Wireless Lan	81xx	v.1.0, v.1.1, and v.1.2

Important:

For ERS 3500 devices, COM 3.0.1 supports discovery, inventory device right-click menus, and EDM plugin only. The COM managers do not discover the ERS 3500 devices.

The earlier versions of ERS devices are also available. However, the official testing has happened against the devices in the list above only.

For the up to date device support information please refer to the Release Notes.

Chapter 14: Appendix Recommendations and deployments

The following sections describe how to resolve Avaya Configuration and Orchestration Manager (COM) problems, and also describe the recommendations and deployments for those errors.

- [COM installation server](#) on page 121
- [Rediscovery of devices](#) on page 121
- [Internet browser Settings](#) on page 122

COM installation server

There may be scenarios in which the Configuration and Orchestration Manager (COM) installation server is in the same local area network (LAN) as devices, or outside the network. Following are some of the recommendations for installing COM server.

- If the COM installation server is outside, then the installation requires VPN secure access to reach the device.
- COM uses several protocols to communicate to the devices and these should be allowed across all the devices.
- Avaya recommends that the COM server chosen is as close as possible to the device, that is, the lesser the hops to access the device the better.
- The TFTP traffic typically does not pass through a firewall, and therefore the TFTP server must run on subnets where the devices are located.

Rediscovery of devices

If you discover devices, add the discovered devices to groups, and then perform additional discoveries to remove the devices; the rediscovered devices appear in red. The rediscovered devices continue to appear in red until you perform another discovery or remove the devices from the device group manager.

Internet browser Settings

Certain security settings in Internet Explorer (IE) do not allow Java script execution. In this case, the login page does not display the login button.

Use the following settings for IE:

- To allow Java script execution, set the IE security settings to at least medium high or lower, as shown in the following figure.

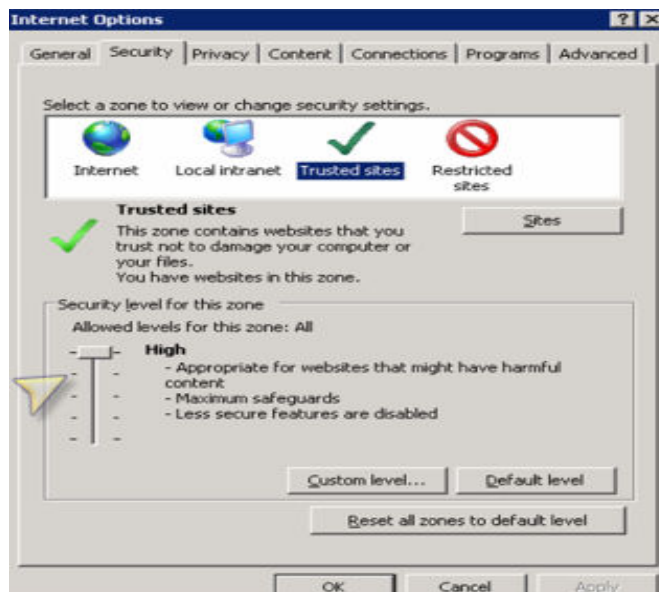


Figure 13: IE settings

- Additional settings for group policies that disable execution of scripts. Use the same functionality in Firefox, if a problem persists.