Avaya Configuration and Orchestration Manager - Using the Product Interfaces

2.3
NN47226-100
04.02
June 2011

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 Web sites 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 Web site: 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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, 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").

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

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks

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 Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: New in this release

The following sections detail what's new in *Avaya Configuration and Orchestration Manager Using the Product Interfaces* (NN47226-100) for Release COM 2.3.

Features

See the following sections for information about feature changes.

VSN Manager

The Virtual Services Network (VSN) Manager is a multielement manager that permits you to configure and view L2 and L3 Shortest Path Bridging MAC (SPBm) throughout the discovered network. You can add, delete, and edit L2 SPBm and L3 SPBm across multiple devices. For more information about the VSN Manager, see VSN Manager on page 77, and *Avaya Configuration and Orchestration Manager Administration—Utilities* (NN47226–600).

Trap Viewer

The Trap viewer tool is added to the Managers panel. For more information about the Trap Viewer, see Trap Viewer on page 77, and the *Avaya Configuration and Orchestration Manager Administration—Utilities* (NN47226–600).

Syslog Viewer

The Syslog viewer is moved from the Trap/Log Manager to the Managers panel. For more information about the Syslog Viewer, see Syslog Viewer on page 77, and *Avaya Configuration and Orchestration Manager Administration — Utilities* (NN47226-600).

VSN Wizard

The Virtual Services Network (VSN) Wizard permits configuration of VSN service VPNs and SPB ISIS infrastructure data. For more information about the VSN Wizard, see Wizards management on page 79, and *Avaya Configuration and Orchestration Manager Administration—Utilities* (NN47226–600).

VSN Template

You can create a Virtual Services Network (VSN) template using the VSN Wizard or the Templates tool. For more information about the VSN template, see Templates management on page 83, and *Avaya Configuration and Orchestration Manager Administration—Utilities* (NN47226–600).

Other changes

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

- Figures on page 6.
- Supported devices on page 7

Figures

Figures in this document are updated.

Supported devices

COM 2.3 supports the following additional devices:

- ERS 8600 v.7.1
- ERS 45xx v.5.5
- Belden L2E Switch v.6.0.02
- Belden L2P Switch v.6.0.02
- Belden L3P Switch v.6.0.02

For more information about supported devices, see Supported devices on page 111.

Chapter 2: Introduction

Avaya Configuration and Orchestration Manager (COM) provides you with an intuitive interface to configure, manage, and provision 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. COM is a management system that manages multiple network devices.

Navigation

Chapter 3: Configuration and Orchestration Manager overview

This chapter provides an overview of the Avaya Configuration and Orchestration Manager (COM) applications.

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

Navigation

Introduction

COM provides you with an intuitive interface to configure, manage, and provision 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.

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

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

To run COM, you do not need Java Runtime Environment (JRE). The JRE 1.5.0.17 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 — Utilities* (NN47226-600).

COM provides topology driven multiuser, multidevice configuration and provisioning features, and off-box element management features (includes COM—EDM management base features).

COM has the following features.

- COM 2.3 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 also 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.

Topology Manager

The main COM window is also referred to as the Topology Manager (TM). The Topology Manager provides a graphical view of a network of devices that support the Bay Networks Autotopology Discovery Protocol or IEEE 802.1ab.

IEEE 802.1ab

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

802.1ab enables stations connected to a LAN to advertise their capabilities to each other, enabling the discovery of physical topology information for network management. 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 to access the information.

802.1ab also makes it possible to discover certain configuration inconsistencies or malfunctions that can result in impaired communications at higher layers. For example, it can be used to discover 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.

Currently, 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, Configuration Orchestration Manager is not restricted to the discovery of Avaya devices: it 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. Configuration Orchestration Manager cannot provide management for these devices.

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

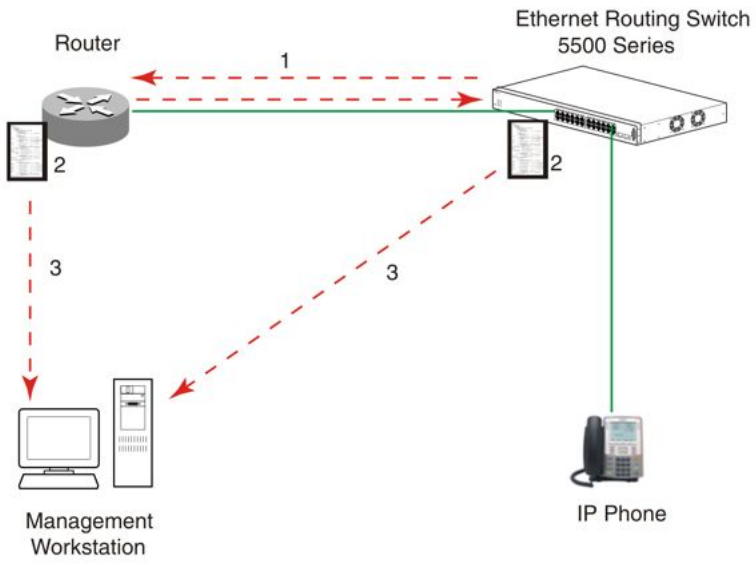


Figure 1: How 802.1ab works

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 details on 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	Allows you to navigate all the panels supported by COM. For more information, see Navigation pane on page 15.
Contents pane	Displays a view of all the discovered devices and their relationship. For more information, see Contents pane on page 17.
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 22.
Links	Allows you to logout, access UCM home, COM details, and view Online Help. For more information, see Links on page 24.

Navigation pane

The Navigation pane is located on the left side of COM main window. The following figure shows the Navigation pane.

Note:

The options that appear in the Navigation panel vary depending on the user tool you select. For more information, see Access Control on page 29 .

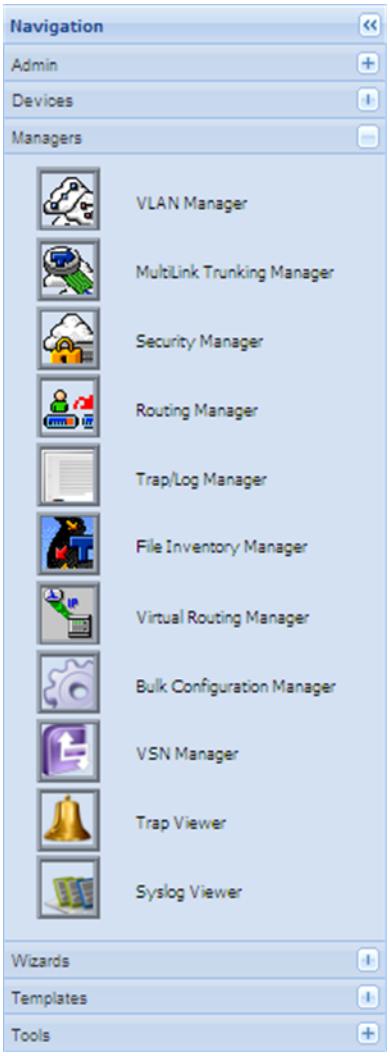


Figure 2: Navigation pane

By default, the Managers panel opens when you access COM.

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

- **Admin**: Contains Access Control, Preferences, Device Credentials, User Management, Licensing, Plugins Inventory, and Audit Log.
- **Devices**: Contains the Device Inventory Manager.
- **Managers**: Contains VLAN Manager, MultiLink Trunking Manager, Security Manager, Routing Manager, Trap/Log Manager, File Inventory Manager, Virtual Routing Manager, Bulk Configuration Manager, Virtual Services Network (VSN) Manager, Trap Viewer, and Syslog Viewer.
- **Wizards**: Contains VLAN, SMLT, and VSN wizards.

- **Templates**: Contains the 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. You can click the (<<) to collapse the Navigation pane.

Contents pane

The Contents pane provides a view of all the discovered devices and their relationship on the Home tab.

The following figure shows the buttons on the Contents pane.

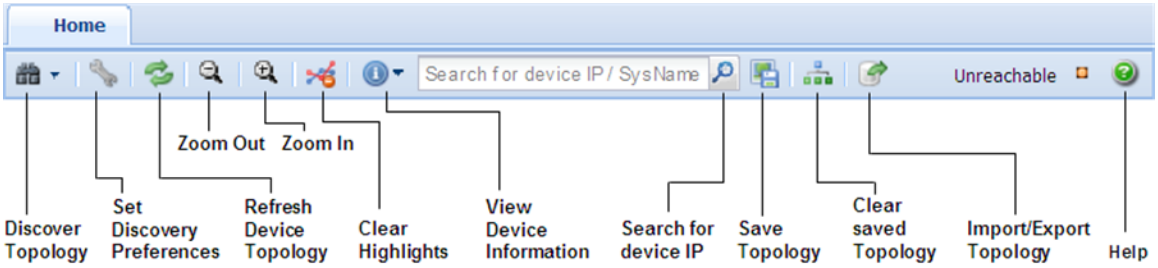


Figure 3: Contents pane toolbar

- **Discover Network Topology**: provides a view of all the discovered devices and their relationship, and includes the single device feature. You can manually add the devices using the add button. These devices are visible on the topology as standalone devices and permit you to launch the element manager and other right click menu functions from the topology view. However, these devices are not available in the multi-element manager functionality.
- **Set Discovery Preferences**: before starting a discovery for the COM system, you can enter the discovery preferences such as Seed and Hop Count.
- **Refresh Device Topology**: refreshes the topology view. It communicates with the server to get the latest discovered devices.
- **Zoom-in, Zoom-out Buttons**: allows you to zoom in or out the topology view.
- **Clear Topology Highlights**: clears the existing highlights on the topology map.
- **View device information**: displays the port names, device types, and Link details like link speed, type, mismatch, and duplex for devices in your topology. Click View device information, and then select the Display port names check box. The following figure shows the View device information menu.

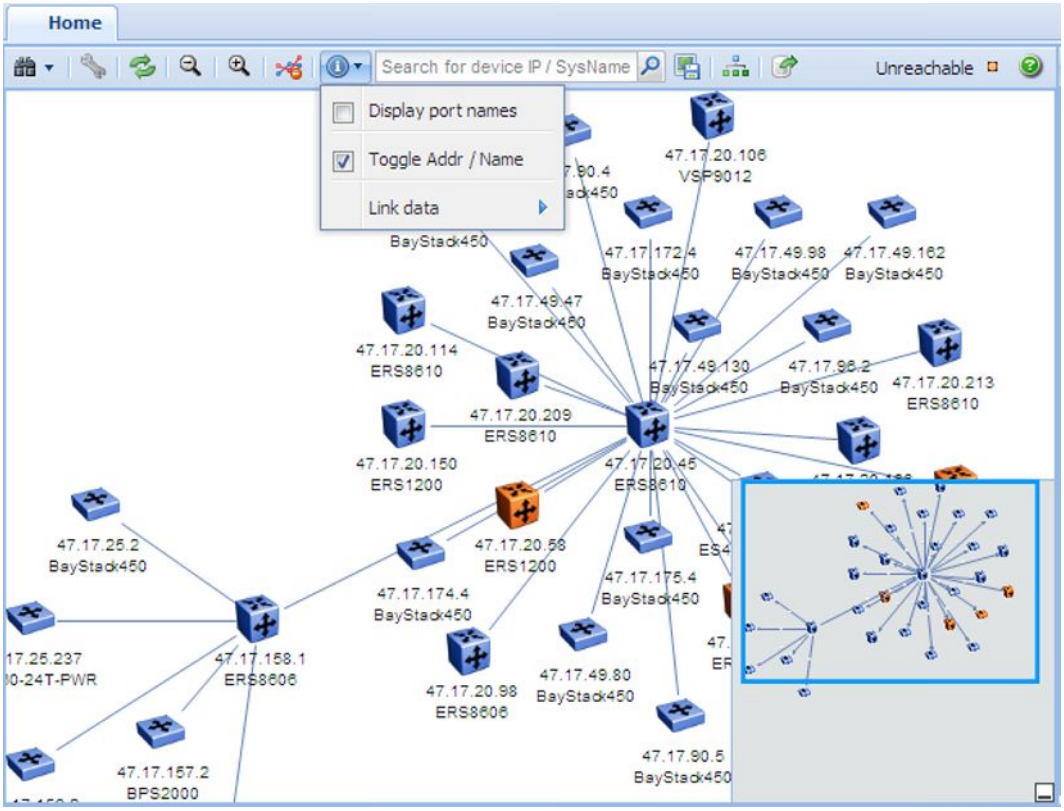


Figure 4: View device information

If a device in your topology has many links (port names or numbers) associated with it, then the topology map can be difficult to read. For example, in the following graphic, the seed IP address is 192.167.1.17; however, a port number (1/24) is overlapping the IP address making the IP address difficult to read. There are also many other overlapping port names. The overlapping port name is not an issue when a port name is shown on a device with a single link. However, multiple links cause the port names to collide or overlap.

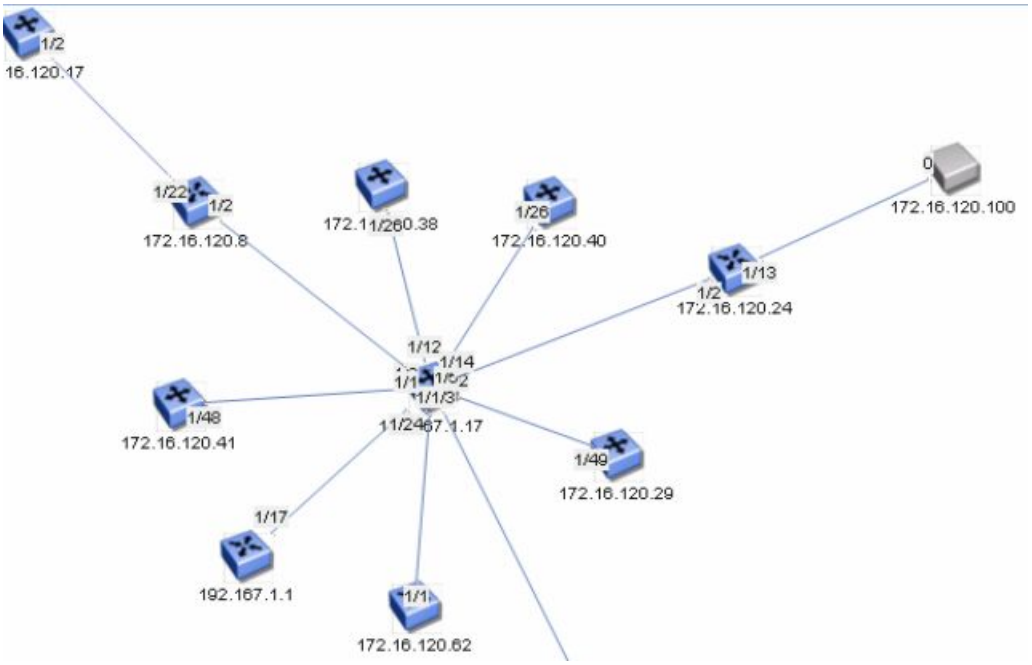


Figure 5: Port names

- **Link data menu**: displays the real-time settings for the interface attributes, and highlights the topology map based on the discovered data. Link data menu is a submenu of Display device information.

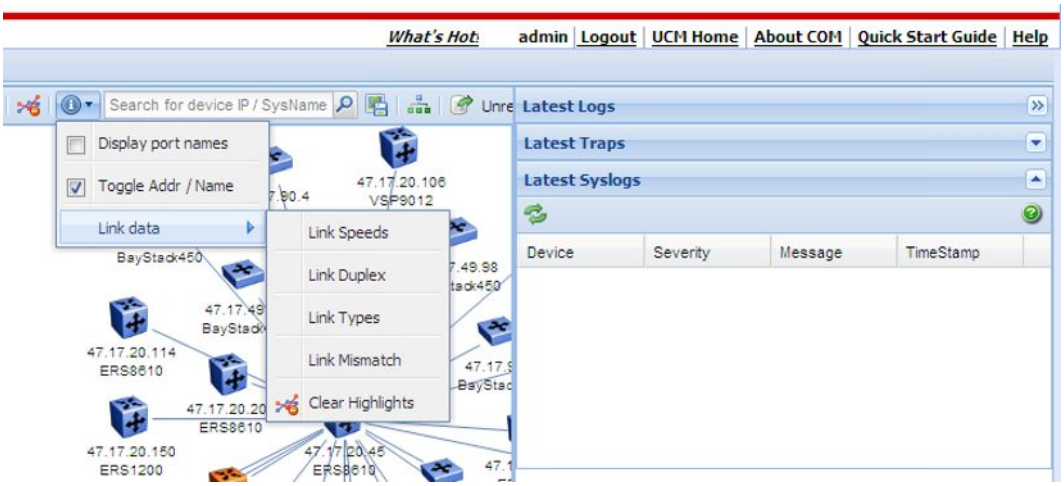


Figure 6: Link associated menu

- **Save topology**: you can 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 COM 2.3, 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 relayout the topology after each discovery
- **Clear Saved Topology**: allows you to return to the topology you previously saved.

- **Import/Export topology**: allows you to export in xml and csv, and import in xml formats.
- **Reachable/Unreachable state**: 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 provided to COM are not correct for the device in the unreachable state.
- **Device navigation window**: you can 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.
- **Search field**: allows you to search and highlight an IP address you are looking for. You can enter an IP address or a partial IP address, and then click Search. The given device with the specified IP address on the map is selected. If you enter a partial IP address, the topology selects the first occurrence of a device that matches the partial IP address, and if you continue to enter, the next one is selected. If the IP address is not found, the search button stops selecting an address.

Important:

If the device is not found, then a Topology dialog box appears showing, "No additional matches found".

Figure 7: Search field

Right-click menu: displays a list of options available to you, when you right-click on the device.

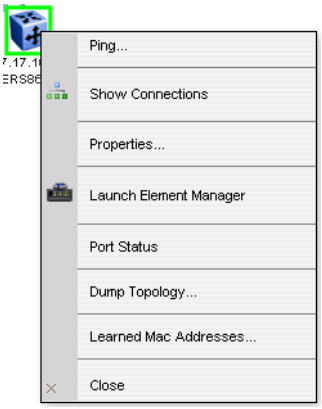


Figure 8: Right-click menu

- **Ping**: allows you to ping the selected device from the server.
- **Show connections**: displays the neighbors of a device on the topology map. It does not display live connections, only what is on the topology map.

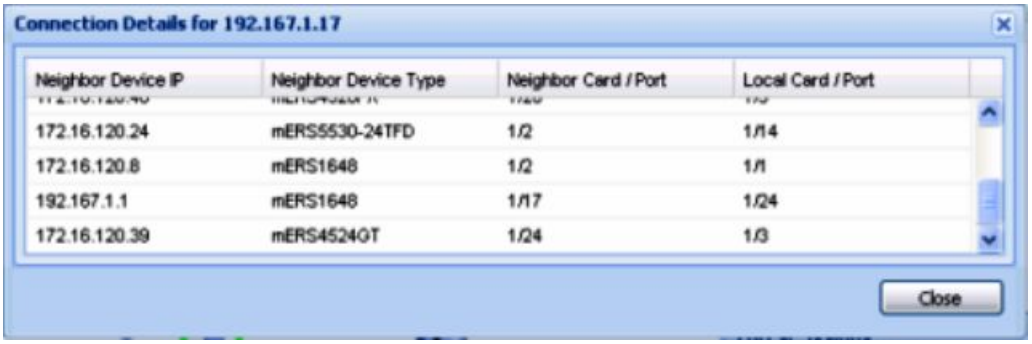


Figure 9: Show connections

- **Properties**: displays properties of the device.

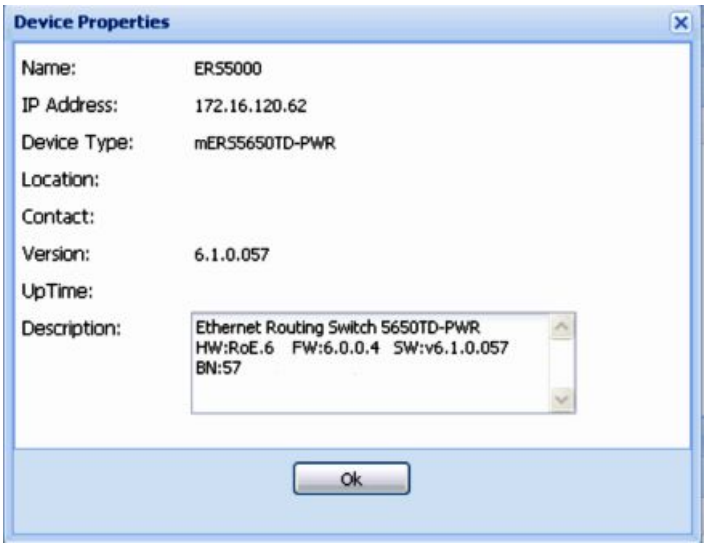


Figure 10: Properties

- **Launch Element Manager**: launches the element manager for the selected device.
- **Dump Topology**: displays the topology based on the real-time queries of devices.
- **Learned Mac Addresses**: displays the learned Mac addresses on the selected device.

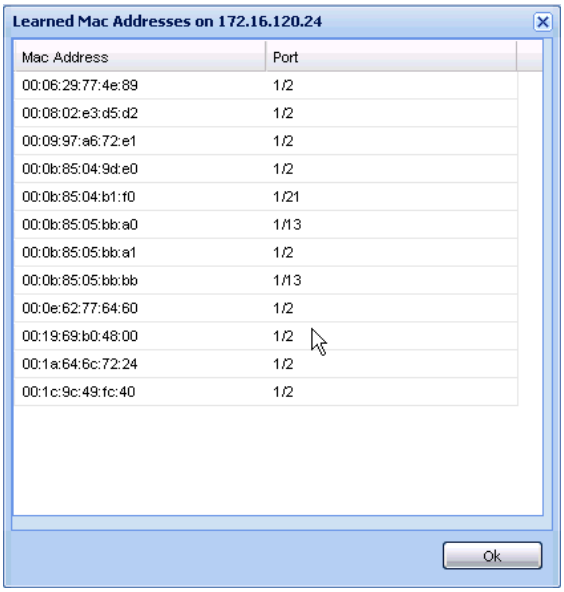


Figure 11: Learned Mac Addresses

- **Port Status**: displays green (the port is up), red (the port is down), and blue (the port is being tested).

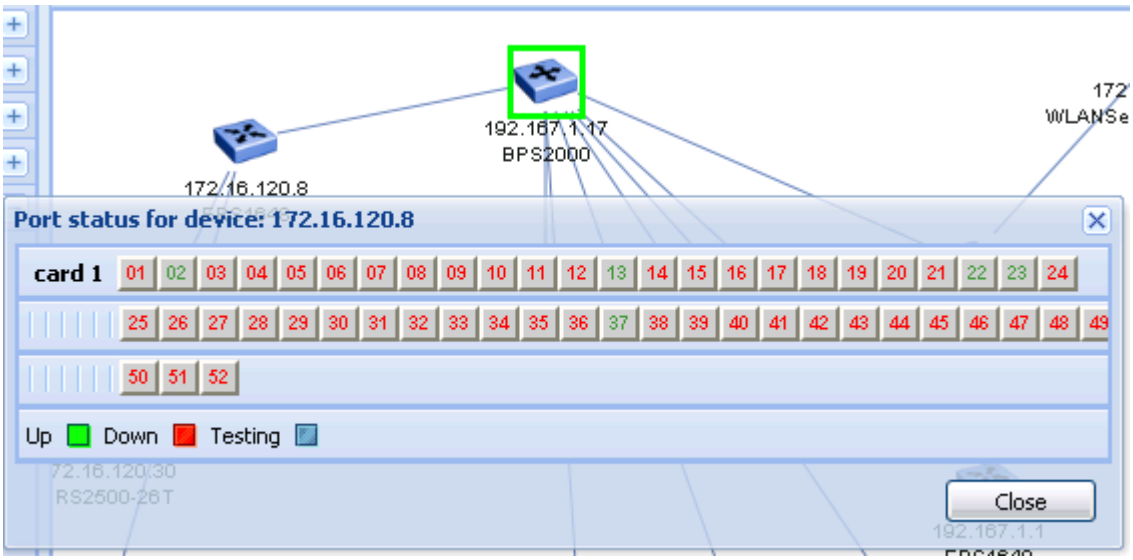


Figure 12: Port status device

Latest Logs pane

Latest Logs pane provides a view of the latest Traps and the latest Syslogs, and displays the last 15 syslogs and traps sent to 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.

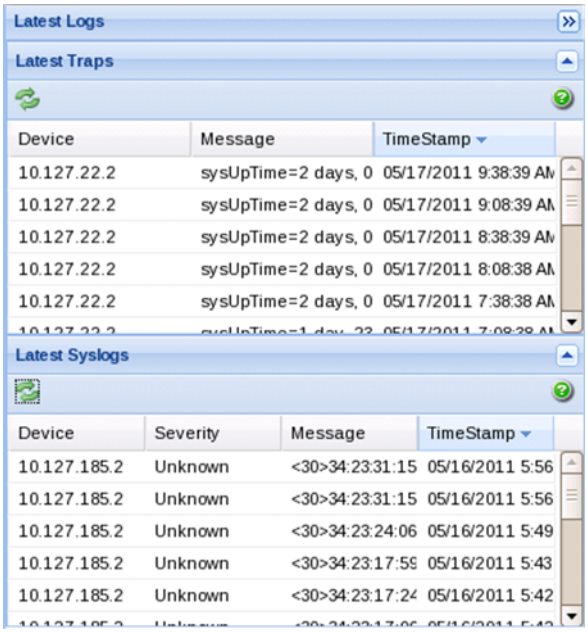


Figure 13: Latest logs pane

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. Severity level, message, and timestamp are provided for each device syslog.

Links

In the upper right corner of COM main window, the following links are available:

- **What's Hot!**
- **admin**: shows 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 displays the version, revision, and build of COM. 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**: The COM quick start guide outlines set up steps that COM administrator should follow after a new COM is installed. It guides the admin through various initial steps like creating users, discovering the network, assigning device and multi-element manager permissions to the users. It also guides the user through the one time setup needed on the client machine.
- **Help**: starts the online help.

The following figure displays COM links.

Figure 14: COM Links

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 25

Logging on to COM

Perform the following procedure to start the COM application.

Prerequisites

- You must install COM.
- You require Internet Explorer 7, or Firefox 3.6 if logging on with a client PC.

Procedure steps

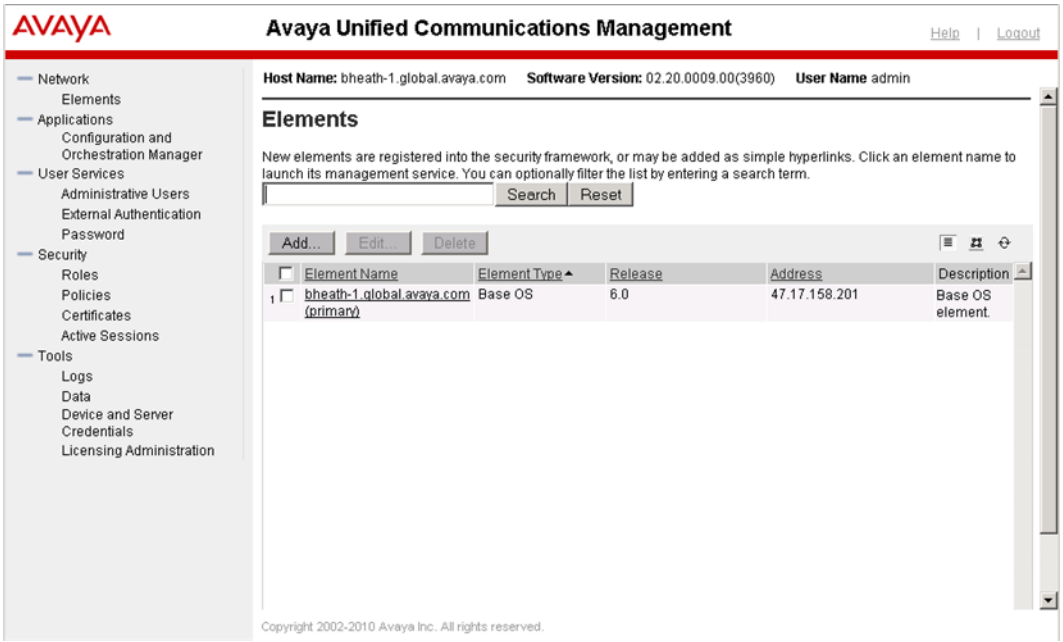
1. Start a Web browser supported by COM.
2. In the **Address** field, enter the Fully Qualified Device Name (FQDN) of the COM server.

   The COM logon screen appears.

3. In the **User ID** field, enter the installed COM user ID.

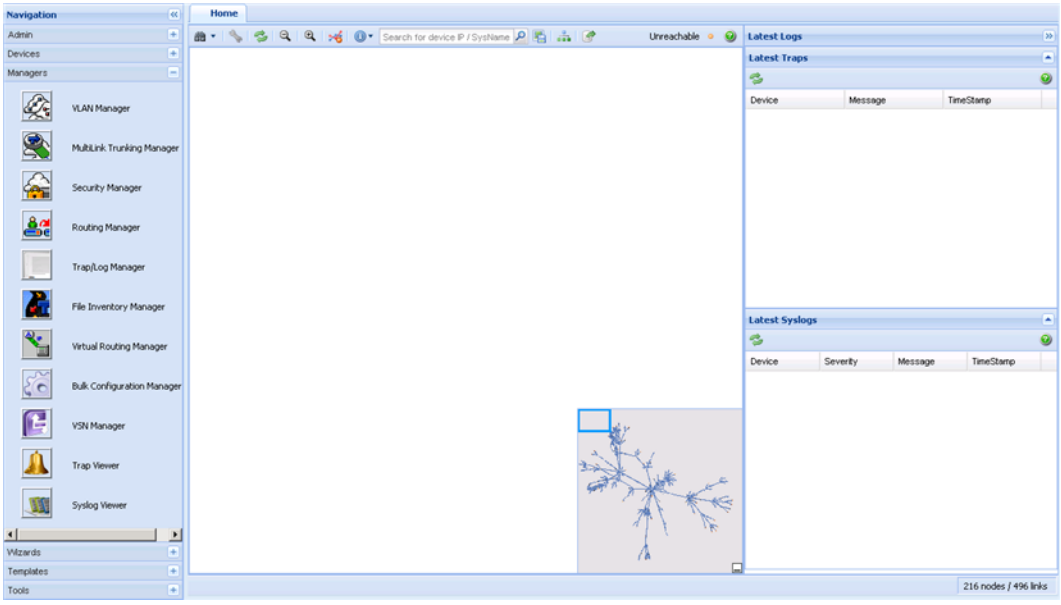
   The default user ID is **admin**.
4. In the **Password** field, enter the installed COM password.
5. Click **Log In**.

   The Unified Communications Management (UCM) home page appears.



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

The COM home page appears.



Chapter 5: Configuration and Orchestration Manager administration

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

Navigation

Access Control

The Access Control service assigns devices to users. Users can only manage the devices assigned to them. 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.

Important:
All the devices discovered by the default Admin user are automatically assigned to this default Admin user only. All other users can use devices that are assigned to them.

The Access Control tab has two tabs:

- Device Assignment
- MultiElement Manager Assignment

See the following sections to manage access control components.

Assigning or unassigning devices

Perform the following procedure to assign devices to the selected COM user or restrict the selected COM user from accessing devices.

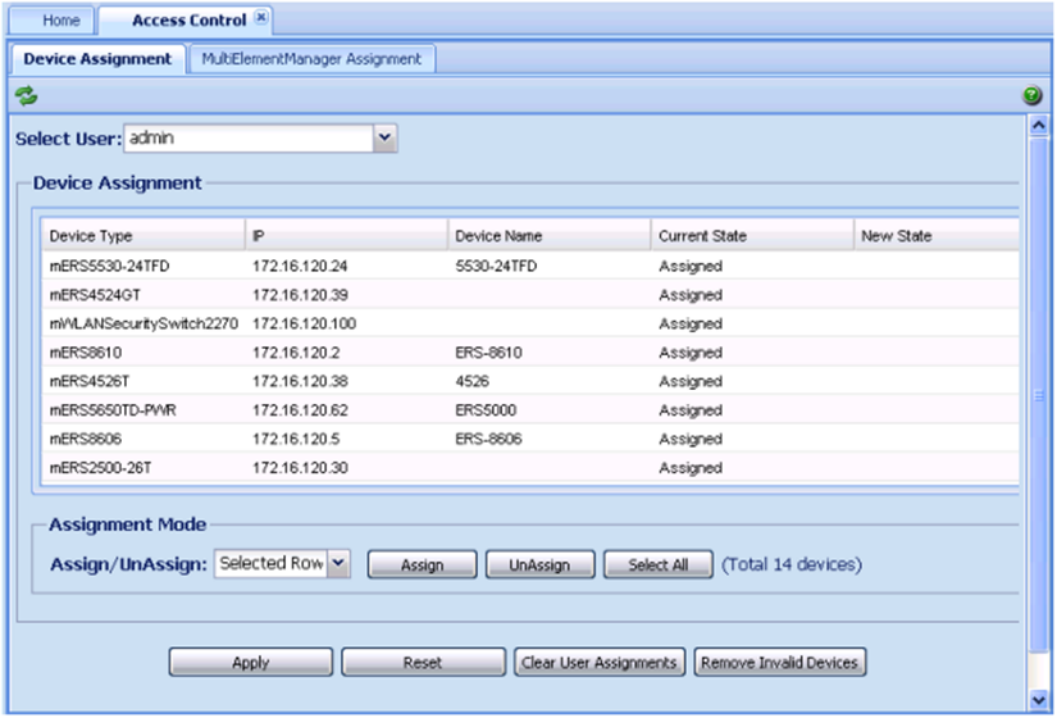
Prerequisites

Ensure that you are logged on to COM as a default admin.

Procedure Steps

1. From the Navigation pane, expand the **Admin** pane, and then click **Access Control**.

   The Access Control tab appears (in the Contents pane) with the Device Assignment tab selected.



2. From the **Select User** list, select the user.

3. From the **Device Assignment** table, select the device names that you want to assign or unassign.
4. In the **Assignment Mode** section, from the **Assign/Unassign** list, select the type of assignment mode.
5. To select all the devices, click **Select All**.
6. Click **Assign** or **UnAssign**.
7. Click **Apply**.

   The Update Status dialog box appears.

Resetting device assignments

Perform the following procedure to reset the assigned devices for the selected 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**.

   The Access Control tab appears (in the Contents pane) with the Device Assignment tab selected.
2. From the **Select User** list, select the user.
3. From the **Device Assignment** table, select the device names that you want to reset.
4. Click **Reset**.

Clearing device assignments

Perform the following procedure to clear device assignments for the selected COM user.

Prerequisites

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

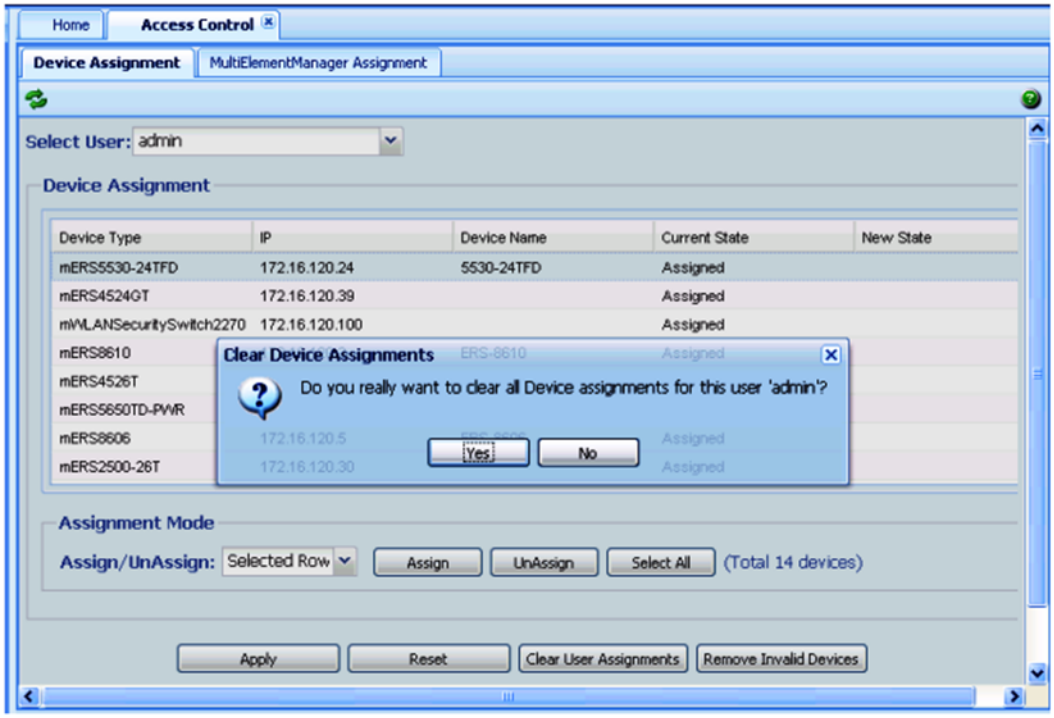
Procedure steps

1. From the Navigation pane, expand the **Admin** pane, and then click **Access Control**.

   The Access Control tab appears (in the Contents pane) with the Device Assignment tab selected.
2. From the **Select User** list, select the user.

3. Click **Clear User Assignments**.

   The Clear Device Assignments dialog box appears.



4. Click **Yes**.

Removing invalid devices

Perform the following procedure to remove invalid devices for the selected 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**.

   The Access Control tab appears (in the Contents pane) with the Device Assignment tab selected.
2. From the **Select User** list, select the user.
3. Click **Remove Invalid Devices**.

   All the invalid devices in the COM server are removed.
4. Click **OK**.

Refreshing the device assignment list

Perform the following procedure to refresh the device assignment list.

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**.

   The Access Control tab appears (in the Contents pane) with the Device Assignment tab selected.
2. From the **Select User** list, select the user.
3. Click **Refresh**.

Assigning MultiElement Manager

Perform the following procedure to assign the MultiElement Manager to the selected COM user.

Prerequisites

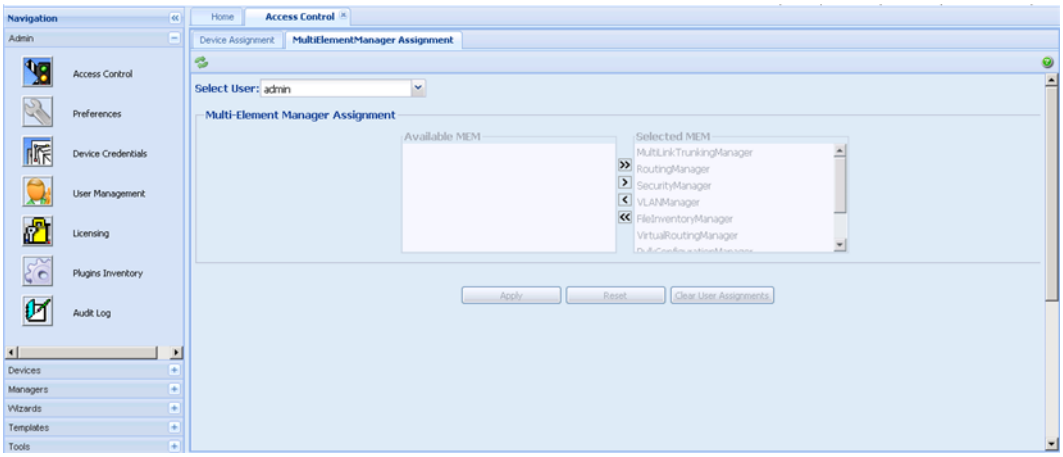
Ensure that you are logged on to COM as an administrator.

Procedure Steps

1. From the Navigation pane, expand the **Admin** pane, and then click **Access Control**.

   The Access Control tab appears (in the Contents pane) with the Device Assignment tab selected.
2. Click the **MultiElementManager Assignment** tab.

   The MultiElementManager tab appears.



3. From the **Select User** list, select the user.
4. In the **Multi-Element Manager** 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 **Right Arrow**.
   - To assign several element managers, press and hold **Ctrl**, select the element manager, release **Ctrl** , and then click **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 **Right Arrow**.
   - To assign all the element managers, click **Double right arrow**.
5. To remove one or more element mangers, select them from the **Selected MEM** list, and then click **Left Arrow**.

   To remove all the element managers, click **Double Left Arrow**.
6. Click **Apply**.

Resetting MultiElement Manager assignment

Perform the following procedure to reset the MultiElement Manager assignment for the selected 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**.

The Access Control tab appears (in the Contents pane) with the Device Assignment tab selected.

2. Click the **MultiElementManager Assignment** tab.
3. From the **Select User** list, select the user.
4. Click **Reset**.

Clearing MultiElement Manager assignments

Perform the following procedure to clear the MultiElement Manager assignments for the selected 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**.

   The Access Control tab appears (in the Contents pane) with the Device Assignment tab selected.
2. Click the **MultiElementManager Assignment** tab.
3. From the **Select User** list, select the user.
4. 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**.

   The Access Control tab appears (in the Contents pane) with the Device Assignment tab selected.
2. Click the **MultiElementManager Assignment** tab.
3. From the **Select User** list, select the user.
4. Click **Refresh**.

Preferences

Preferences manages a set of 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 36
- Discovering devices on page 37
- Configuring general system preferences on page 38
- Configuring logging information on page 39

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 muse use the global preference ENABLE_MANAGER_PERSISTENCE. 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 some configuration 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 saving happens automatically.

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

- MLT Manager
- VLAN Manager
- Routing Manager

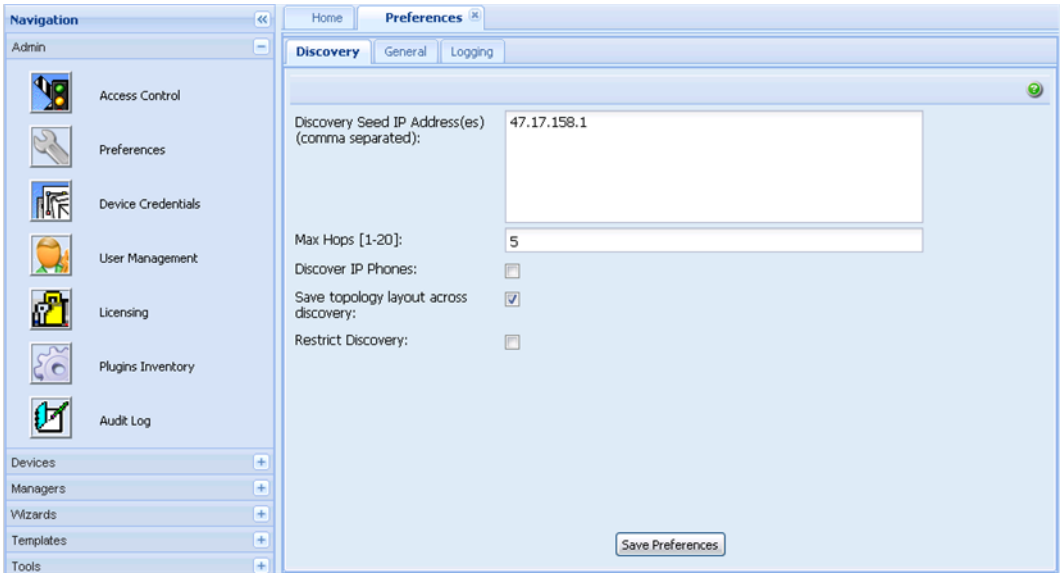
Discovering devices

Perform the following procedure to discover devices for COM.

Procedure steps

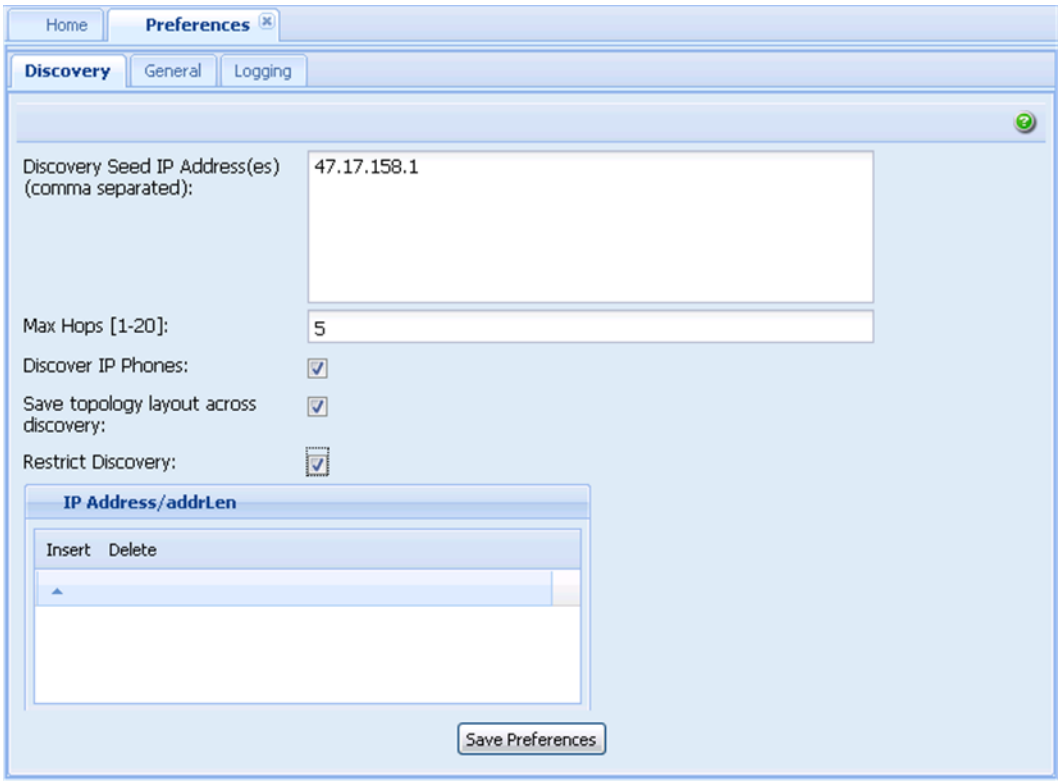
1. From the Navigation pane, open **Admin** and then select **Preferences**.

   The Preferences dialog box appears in the Contents pane.



2. In the **Discovery Seeds** field, enter the IP address of one or more devices in the network. Separate multiple IP addresses with a comma.
3. In the **Max Hops** field, enter the maximum number of hops.
4. Check the **Discover IP Phones** check box to discover the IP phones and to appear in the topology map.
5. Check the **Save topology layout across discovery** check box to save the topology layout.
6. In the **Restrict Discovery** check box, check the check box to restrict device discovery to only the devices entered in the subnets.

If Restrict Discovery check box is selected, then the IP Address/addrLen dialog box appears.



7. Click **Insert** to enter the IP addresses.
8. To delete an IP address, select the required row and click **Delete**.
9. Click **Save Preferences**.

Configuring general system preferences

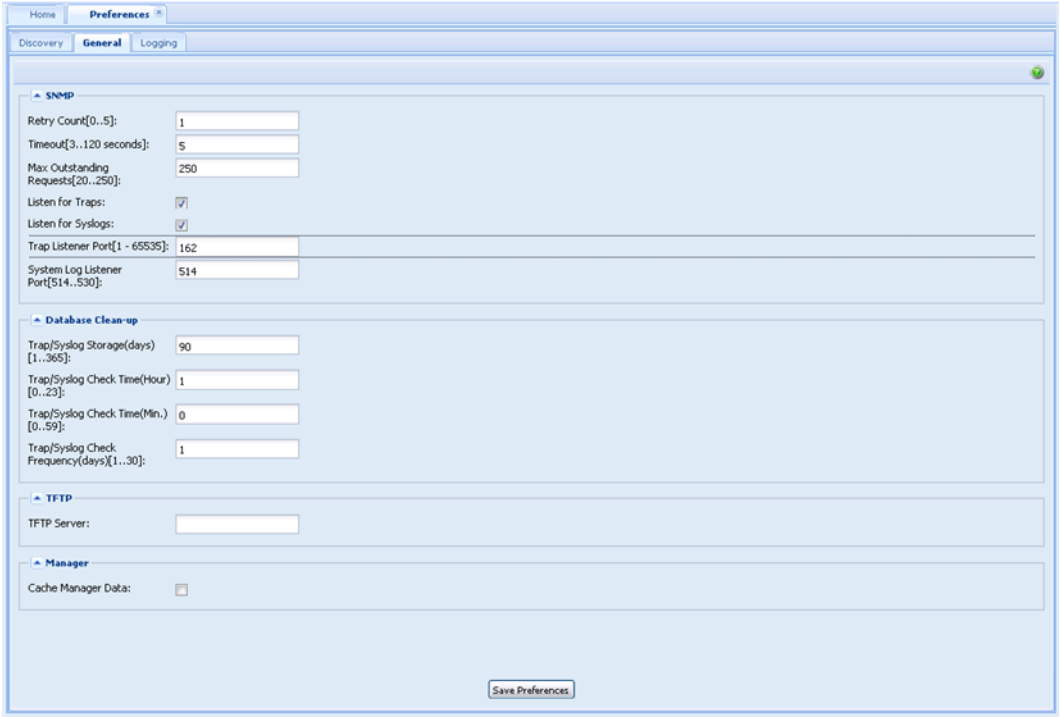
Perform the following procedure to configure the general system preferences.

Procedure steps

1. From the Navigation pane, open **Admin** and then select **Preferences**.

   The Preferences dialog box appears in the Contents pane.
2. Click **General**.

   The General dialog box appears.



3. Enter all the fields in **SNMP**, **Database Clean-up**, and **TFTP** panes as appropriate.
4. Click **Save Preferences**.

Configuring logging information

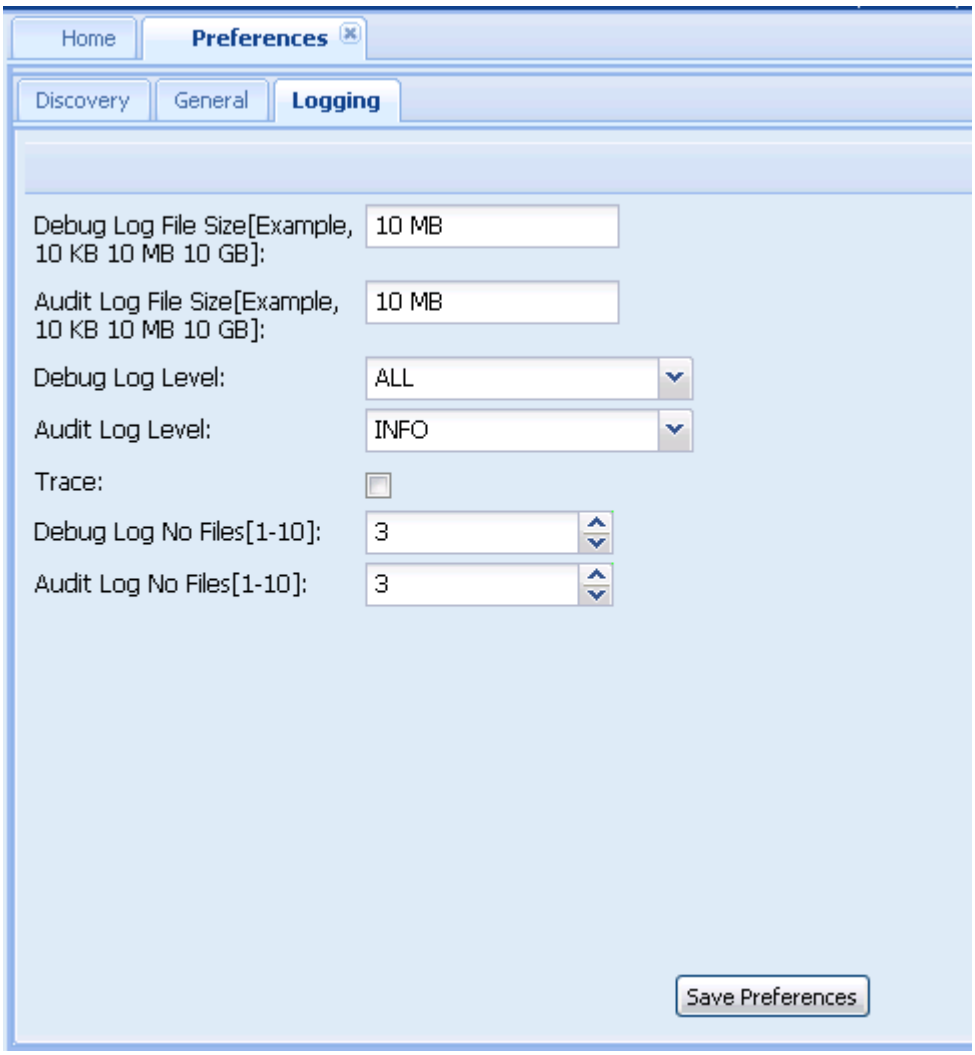
Perform the following procedure to configure logging.

Procedure steps

1. From the Navigation pane, open **Admin** and then select **Preferences**.

   The Preferences dialog box appears in the Contents pane.
2. Click **Logging**.

   The Logging dialog box appears.



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

Job aid

The following table describes the fields of Preference tabs.

Table 2: Preferences fields

Tab	Item	Description
Discovery	Discovery Seed IP Address(es) (comma separated)	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 *Avaya Configuration and Orchestration Manager Administration — Utilities* (NN47226-600).

Tab	Item	Description
		Important: 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.
	Discover IP Phones	If selected, IP phones are discovered and appear in the topology map.
	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, 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, COM waits before trying to connect to a device again. The default value is 5.
	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 Syslogs	If checked, COM receives logs for all the devices managed through COM.
	System Log Listener Port[514..530]	The port on the COM server where the COM software listens for syslogs.
General Database Clean-up panel	Trap/Syslog Storage (days) [1..365]	The number of days, between 1 and 365, 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, 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, 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, COM tries to connect to Trap/Syslog storage to purge the database. The default value is 90.

Tab	Item	Description
General TFTP panel	TFTP Server	Allows you to enter the IP address of the default TFTP 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 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.
Logging	Debug Log File Size [Example, 10 KB 10 MB 10 GB]	The user specifies the Debug Log File Size. The default value is 10 MB.
	Audit Log File Size [Example, 10 KB 10 MB 10 GB]	The user specifies the Audit Log File Size. The default value is 10 MB.
	Debug Log Level	The Debug Log Level is specified by the user The default value is ALL.
	Audit Log Level	The Audit Log Level is specified by the user. The default value is INFO.
	Trace	If checked, additional SNMP information is written to COM error log, and can provide assistance in troubleshooting. **Important:** Selecting Trace can slightly slow down performance as extra information is gathered
	Debug Log No Files[1–10]	The number of files which are debugged. The default value is 3.
	Audit Log No Files[1–10]	The number of files which are audited. The default value is 3.

Device credentials

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

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

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. COM also requires that you enter telnet credentials for the FIM module. The BCM module within COM requires either Telnet and SSH credentials to be available

The following table lists the categories of credential information that can be managed in the Device and Server Credentials Editor.

Table 3: Device and Server Credentials Editor fields

Credential information	Attributes
Name	Credential set name
IP Address or Range	Device/Server IP Address or Address Range
SNMPv1/v2	Read Community Write Community
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
FTP	FTP User name FTP Password FTP Port
SSH	SSH User name SSH Password SSH Port
CIM-XML	CIM User name CIM Password
RLogin	RLogin User name RLogin Password

Credential information	Attributes
Windows Server	Windows User name Windows Password Windows Domain

Navigation

- Adding a credential set on page 44
- Adding a credential set for SNMPv3 on page 45
- Deleting a credential set on page 47
- Editing a credential set on page 47
- Importing a credential set on page 49
- Exporting a credential set on page 50

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.

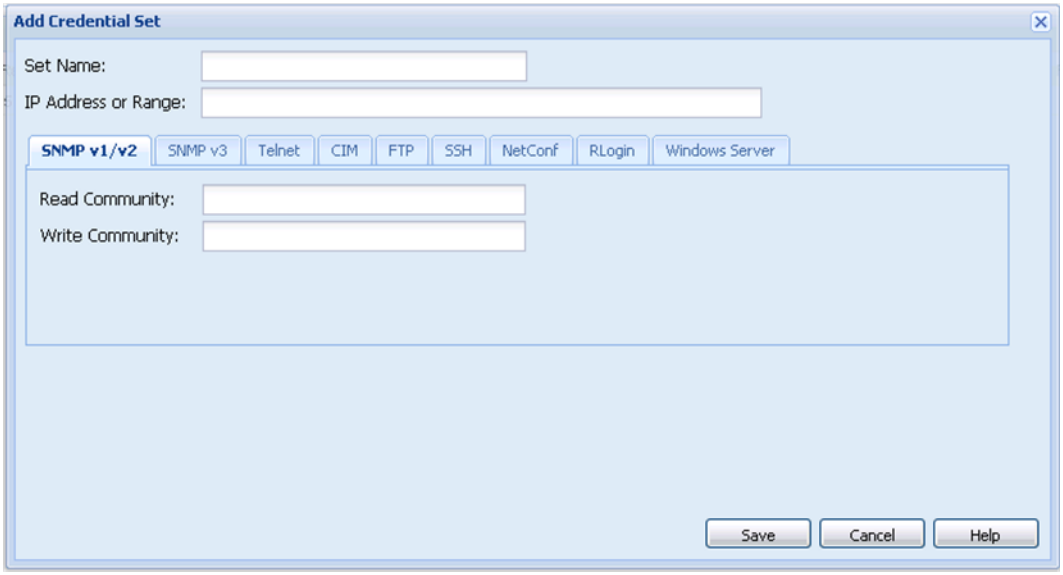
Procedure steps

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

   The Device and Server Credentials Editor page appears.

2. Click **Add Credential**.

   The Add Credential Set dialog box appears.



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 3: Device and Server Credentials Editor fields on page 43.

   Each tab corresponds to an authentication protocol. The information you enter depends on the type of authentication your device uses.
6. Click **Save**. The credential set appears in the panel.

Adding a credential set for SNMPv3

Perform the following procedure to add credentials for SNMP v3.

Procedure steps

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

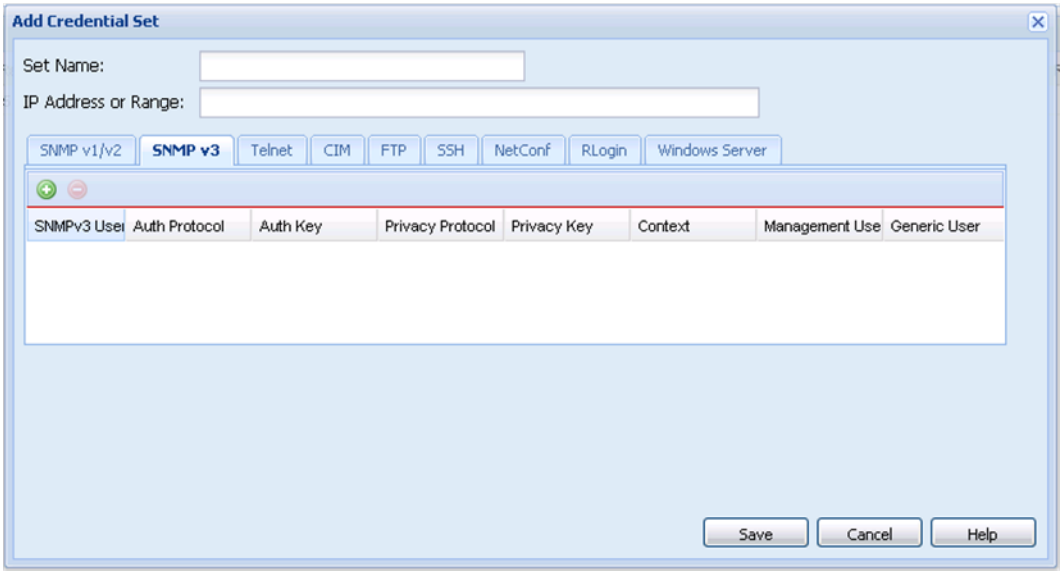
   The Device and Server Credentials Editor page appears.

2. Click **Add Credential**.

   The Add Credential Set dialog box appears.

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**.

   The SNMP v3 dialog box appears.



6. 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 have to associate the device snmpv3 user to a UCM user, otherwise the entry will not take effect.

Generic User: Ensure this field is set to true.

7. Click **Save**. The credential set appears in the panel.

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**.

   The Device and Server Credentials Editor page appears.

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)**. After you are prompted to confirm the deletion of 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.

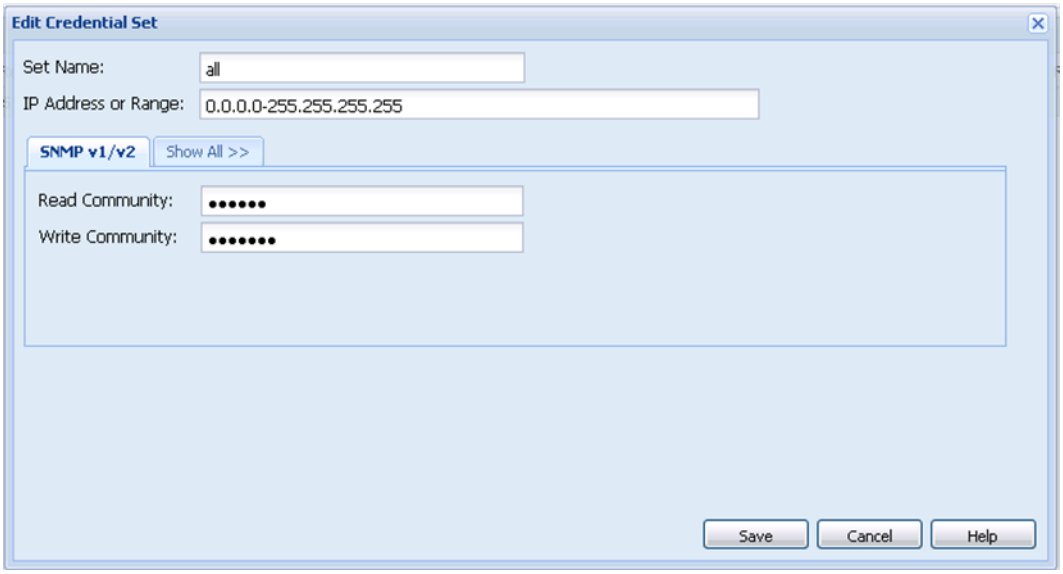
Procedure steps

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

The Device and Server Credentials Editor page appears.

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

   The Edit Credential Set dialog box appears.



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**.

   All specified IP addresses are validated after saving the changes.

Importing a credential set

Perform the following procedure to import the credential set to the UCM.

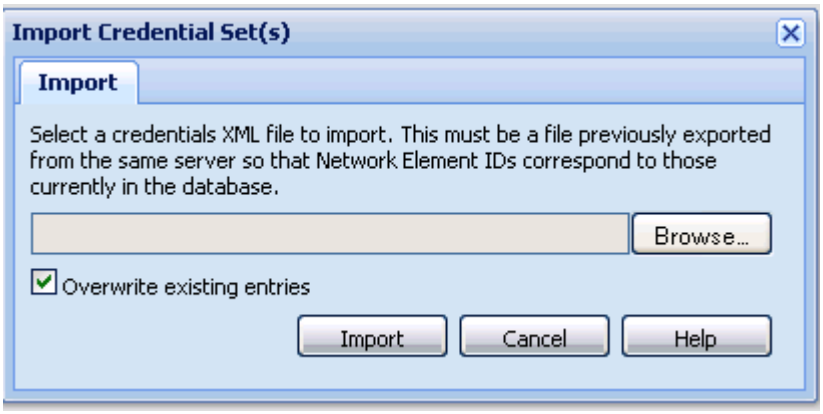
Procedure steps

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

   The Device and Server Credentials Editor page appears.

2. Click **Import Credentials**.

   The Import Credential Set(s) dialog box appears.



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 credential set from the UCM to a local XML file.

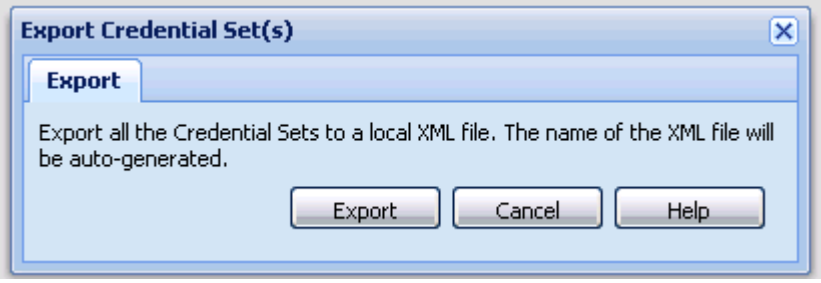
Procedure steps

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

   The Device and Server Credentials Editor page appears.

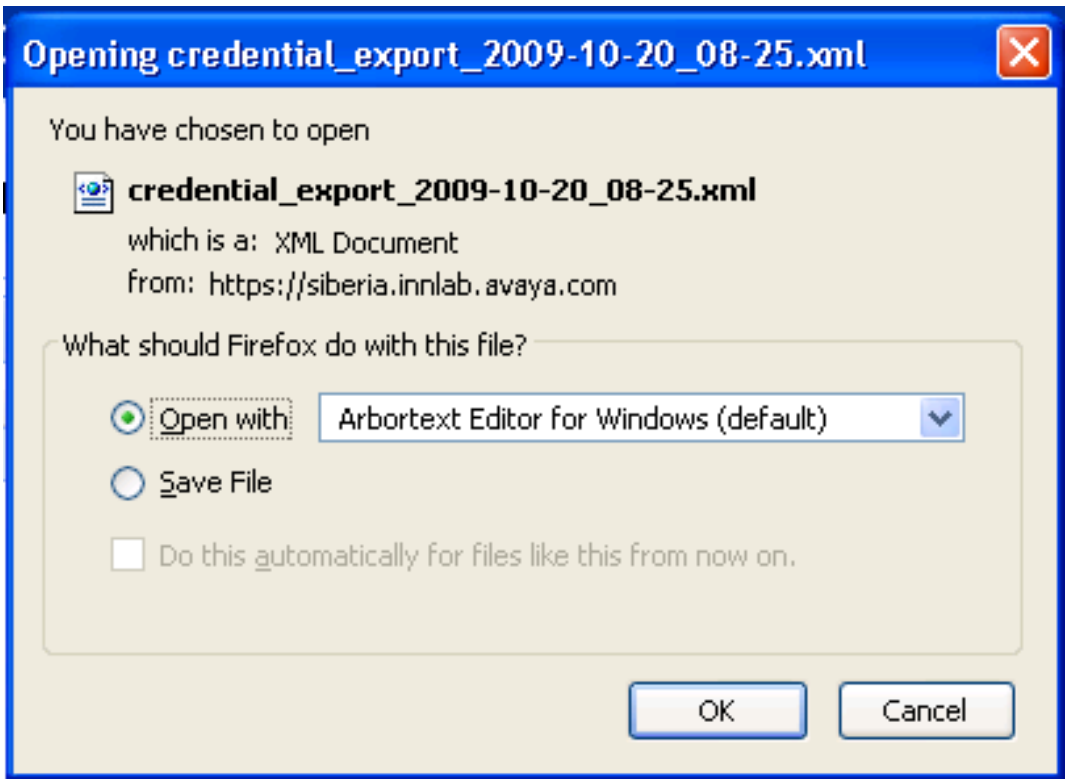
2. Click **Export Credentials**.

   The Export Credential Set(s) dialog box appears.



3. Click **Export**. The Credential Sets exports to a local XML file. The name of the XML file is autogenerated.

   The File Download dialog box appears.



4. Click **Save**.

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 51
- Viewing existing users on page 54
- Adding a new local or external user on page 54
- Disabling an user on page 57
- Deleting a user on page 57

Avaya UCM role

COM supports the following Avaya Unified Communications Management (UCM) user roles:

- NetworkAdministrator
- UCMSystemAdministrator
- UCMOperator

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

Table 4: UCM user roles on UCM and COM components

Component	NetworkAdministrator	UCMSystemAdministrator	UCMOperator
Main Page	Yes	Yes	Yes
Security Management Page (Quantum Page)	Yes (users, roles, sessions, and policies management)	Yes (can only change user's own password)	Yes (can only change user's own password)
Device and Server Credentials Page	Yes (read and write)	Yes (read only)	Yes (read only)
Backup and Restore Commands (no UI; only run from command line)	Yes (as long as OS user is in Administrators or root group)	Yes (as long as OS user is in Administrators or root group)	Yes (as long as OS user is in Administrators or root group)
License Page	Yes	Yes	Yes (read only)

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

Table 5: Functionality of UCM roles on COM

Functionality	Full application license / UserRole = NetworkAdministrator (default admin user)	Full application license / UserRole = UCMSystemAdmin	Full 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

Functionality	Full application license / UserRole = NetworkAdministrator (default admin user)	Full application license / UserRole = UCMSystemAdmin	Full application License/ UserRole = Operator
Plugin Launch	Yes	Yes	Yes
User Management	Yes	No	No
Device Assignment to User	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
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 run from command line)	Yes	Yes	No
Wizard, template and scheduler	Yes	Yes	Yes, if access to relevant manager has been provided

Viewing existing users

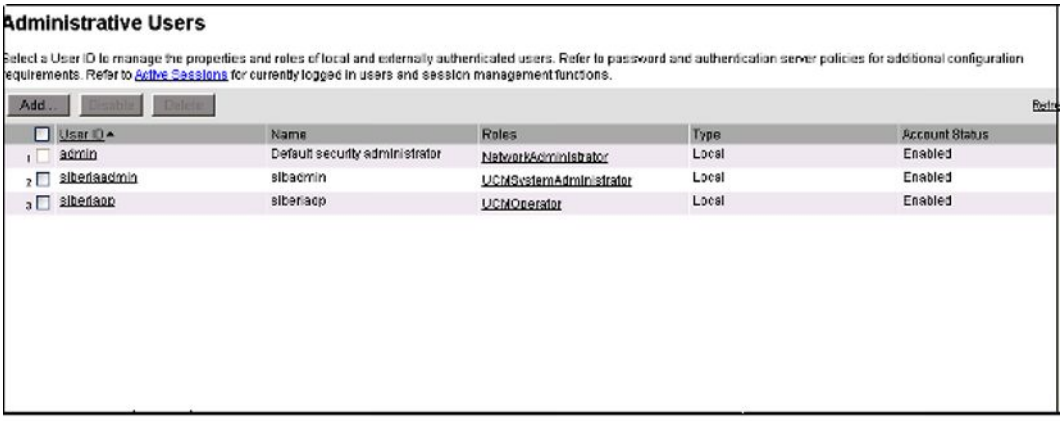
Perform the following procedure to view the users who are configured for UCM access.

Procedure steps

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

   The Administrative Users page appears.

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



2. View the information for existing users.

Adding a new local or external user

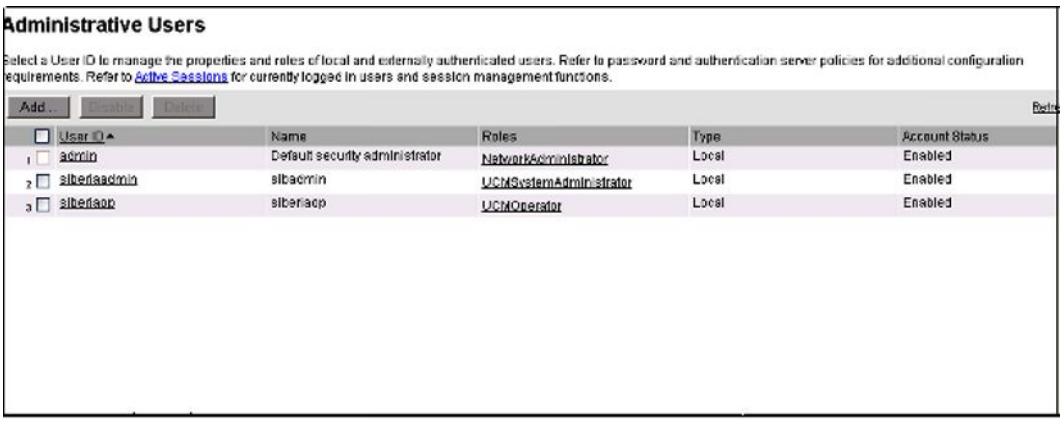
Perform the following procedure to create a new user of UCM and to assign roles to the new user.

Procedure steps

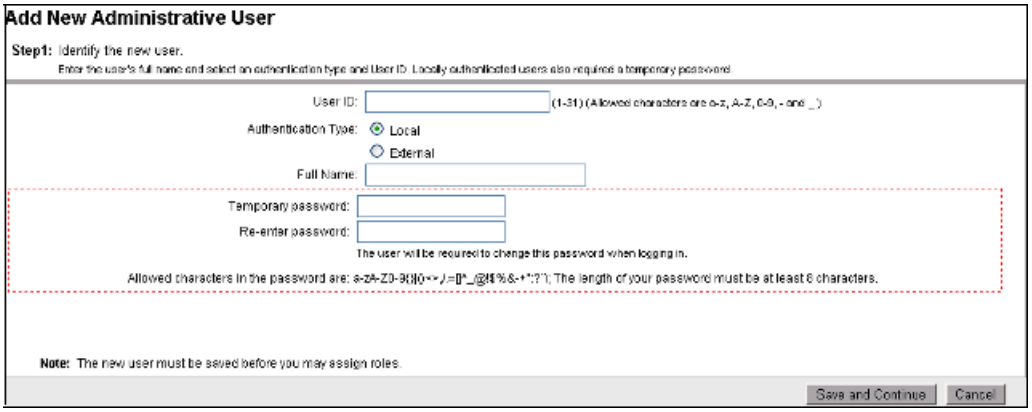
1. In the Navigation pane, expand **Admin**, and then click **User Management**.

   The Administrative Users page appears.

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



2. Click **Add**. The Add New Administrative User page appears.



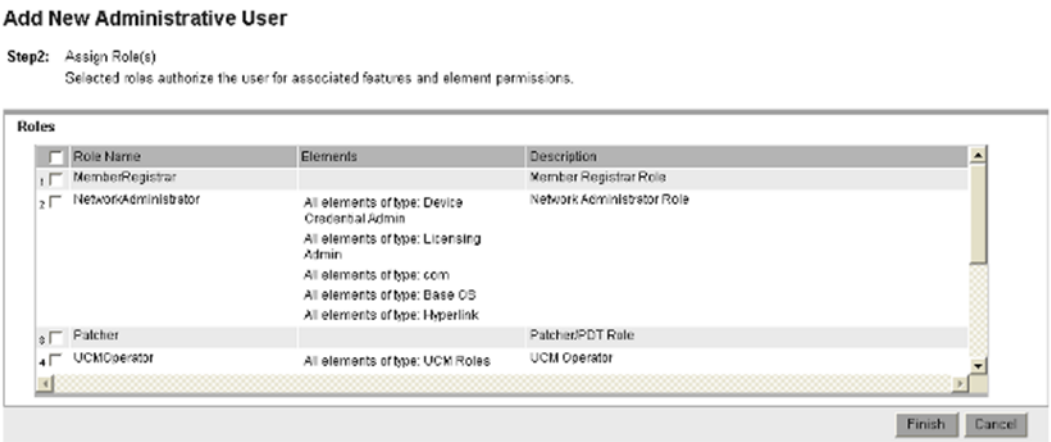
3. In the **User ID** field, enter the user ID.
4. In the **Authentication Type** option, select the user type.
5. In the **Full Name** field, enter the full name of the user.
6. In the **Temporary password** field, enter the temporary password.

Important:

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

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

   The Add New Administrative User Step 2 page appears.



8. In the **Role Name** column, select the **Role Name** check boxes 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	ID of the user. This field can accept 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 an user

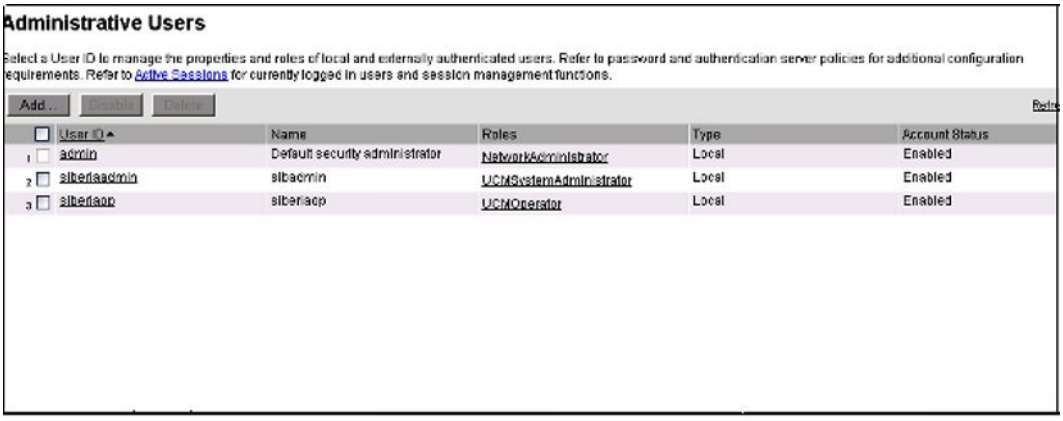
Perform the following procedure to disable the user in the UCM network.

Procedure steps

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

   The Administrative Users page appears.

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



2. In the **User ID**, select the User ID check box that you want to disable, and then click **Disable**. The Account Status for the selected user changes to Disabled.

Deleting a user

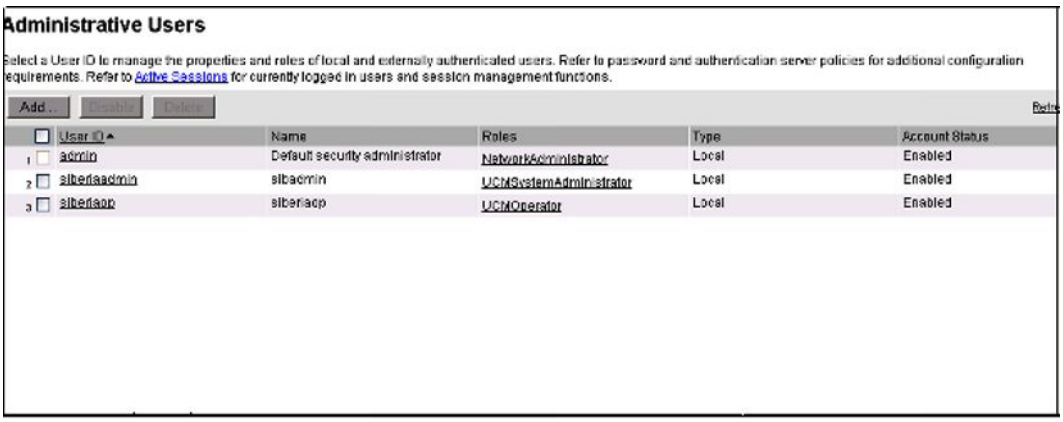
Perform the following procedure to delete a user in the UCM network.

Procedure steps

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

   The Administrative Users page appears.

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



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

   The Delete User dialog box appears.

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

   Important:
   Users cannot delete their own account.

Licensing

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

Navigation

- Adding a license on page 58
- Exporting a license on page 59
- Generating a licensing report on page 60
- Refreshing the license information on page 60

Adding a license

Perform the following procedure to add a license.

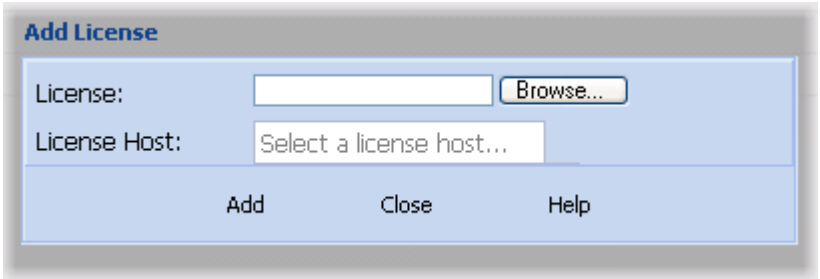
Procedure steps

1. In the Navigation pane, expand **Admin** panel, select **Licensing**.

   The Licensing Administration page appears.

2. Click **Add License**.

   The Add License dialog box appears.



3. 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 **Admin** panel, and then click **Licensing**.

   The Licensing Administration page appears.
2. In the product name table, select the product license to be exported.
3. Click **Export License**.

   The File Download dialog box appears.
4. Click **Save**.

   The required product license is exported.

Generating a licensing report

Perform the following procedure to generate a licensing report.

Procedure steps

1. In the Navigation pane, expand **Admin** panel, and then click **Licensing**.

   The Licensing Administration page appears.
2. In the product name table, select the product license to be exported.
3. Click **Report**.

   The File Download dialog box appears.

4. Click **Save** to save the license report.

Refreshing the license information

Perform the following procedure to refresh the license information.

Procedure steps

1. In the Navigation pane, expand **Admin** panel, and then click **Licensing**.

   The Licensing Administration page appears.
2. In the product name table, select the product license to be exported.
3. Click **Refresh**.

Plugins inventory

The EDM plugin is a device plugin for a device version or type that you can install on an installed COM base. Plugins can be installed on Base or Complete application license. The user of the Network Administrator and UCM System Administrator roles are allowed to do the Plugin management. You can install, uninstall, or view the EDM Plugin by accessing the Plugins Inventory.

EDM plugins serve the purpose of offering Device Management capabilities. Thus, 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 are a browser-based solution, that are launched via device inventory or from the topology map. Right click on a device to launch Element Manager. EDM plugins are reused from the Embedded EDM (Element Manager) that is made available in all the devices.

The EDM Plugin Inventory appears with a table containing all the installed Plugins on the COM server. Each row in the table depicts an EDM plugin, specifying which device type and version is run with the Plugin and also a list of supported device names.

Navigation

- Downloading EDM plugin on page 61
- Installing EDM plugin on page 62
- Uninstalling EDM plugin on page 63
- Refreshing the plugin inventory table on page 64
- Selecting the EDM preferences on page 64

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 COM server.

Procedure steps

1. Open Avaya support site from the Web browser and select EDM Plugins section in http://support.avaya.com.
2. Download **EDM Plugin** for a specific device type and version.
3. 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 EDM plugin on 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/.

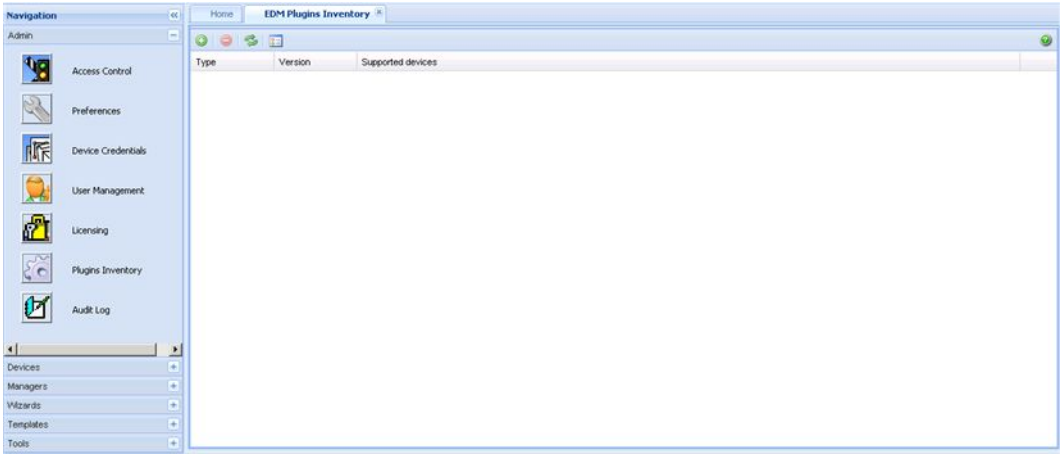
Prerequisites

- 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

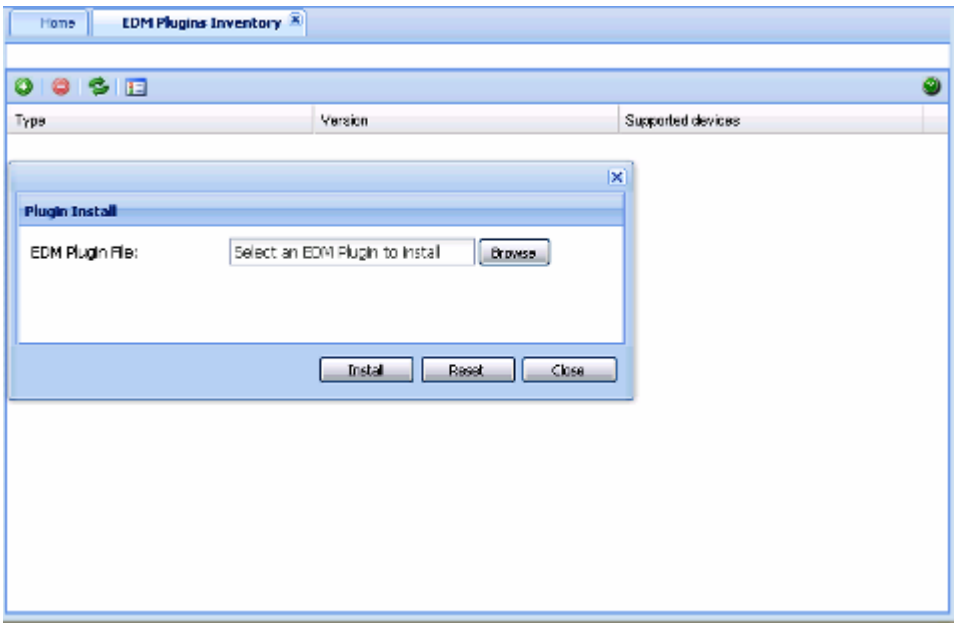
1. Download **EDM plugin** using the procedure, Downloading EDM plugin on page 61.
2. From the Navigation pane, expand the **Admin** pane, and then click **Plugins Inventory**.

   The EDM Plugins tab appears in the Contents pane.



3. Click **Install Plugin**.

   The Plugin Install dialog box appears.



4. To select the EDM Plugin file, click **Browse**. The file upload dialog box appears.
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 a EDM plugin from COM.

The uninstallation process deletes the war file from the JBoss deploy folder, and removes information related to the plugin from the EDMsupportedDevices.xml file and also deletes the mib.dat file used by this 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**.

The EDM Plugins tab appears in the Contents pane.

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 done successfully, the message "EDM Plugin uninstall" successful appears or an error message appears describing 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 COM as an administrator.

Procedure Steps

1. Download **EDM plugin** using the procedure, Downloading EDM plugin on page 61.
2. From the Navigation pane, expand the Admin pane, and then click **Plugins Inventory**.

   The EDM Plugins tab appears in the Contents pane.
3. From the toolbar, click **Refresh Plugin Inventory**.

   The Plugin Inventory table refreshes.

Selecting the EDM preferences

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

Prerequisites

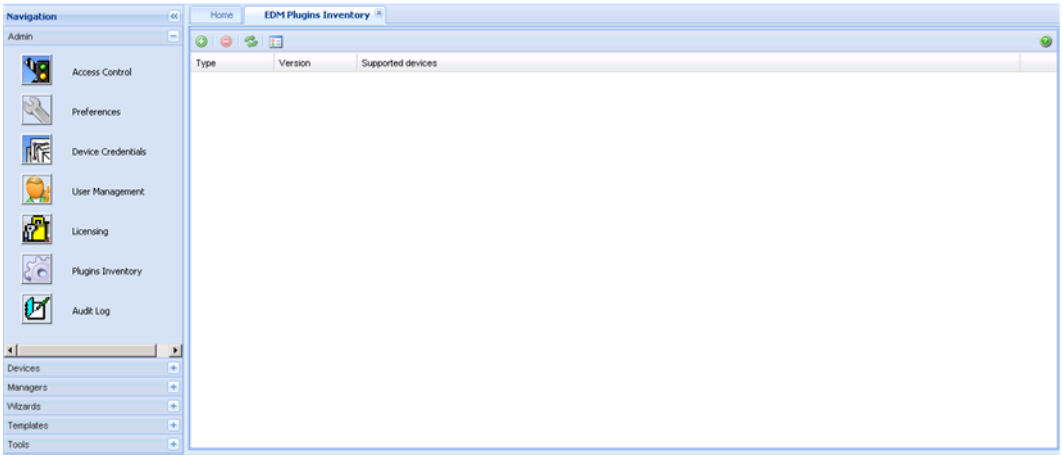
- You must have Network administrator role or UCM system administrator role rights to access the Plugins Inventory.
- Ensure that you log on to COM as an administrator.

Procedure Steps

1. Download **EDM plugin** using the procedure, Downloading EDM plugin on page 61.
2. From the Navigation pane, expand the Admin pane, and then click **Plugins Inventory**.

   The EDM Plugins tab appears in the Contents pane.
3. From the toolbar, click **EDM Preferences**.

   The EDM Preferences dialog box appears.



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

   By default the Use EDM Plugin when launching Single Element Manager checkbox is checked.

Important:

If you choose to uncheck the Use EDM Plugin when launching Single Element Manager check box, please note that it may cause performance issues in the device.

Click **Save**.

Audit log

All the managers including Topology and Discovery send log messages to audit and debug logs.

Navigation

- Launching the audit log on page 66
- Refreshing audit logs on page 66

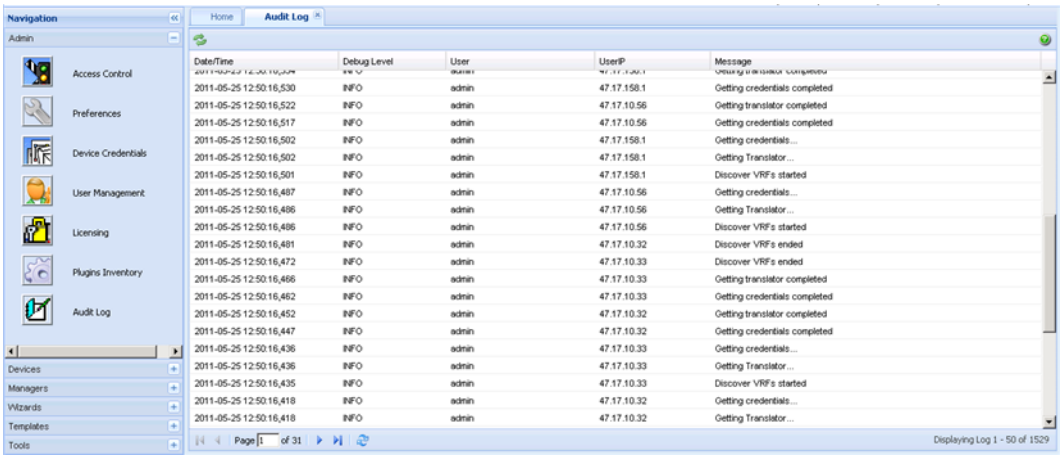
Launching the audit log

Perform the following procedure to start the audit log.

Procedure steps

From the Navigation pane, expand the Admin panel, and then click **Audit Log**.

The Audit Log dialog box appears.



Job aid

The following table shows the Audit Log tabs.

Table 6: Audit log tabs

Tab	Description
Date/Time	The date and time of the Audit Log files
Debug level	The Debug level (Default INFO/ERROR)
User	The logged in user name
UserIP	The User IP address
Message	The log file creates a message

Refreshing audit logs

Perform the following procedure to refresh the audit logs.

Procedure steps

1. From the Navigation pane, expand the Admin pane, and then click **Audit Log**.

   The Audit Log dialog box appears.
2. Click **Refresh**.

   The audit log details are refreshed.

Chapter 6: Devices management

The Device Inventory Manager lets you manage the Avaya Configuration and Orchestration Manager (COM) inventory. COM 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.

The following figure shows the Device Inventory dialog box.

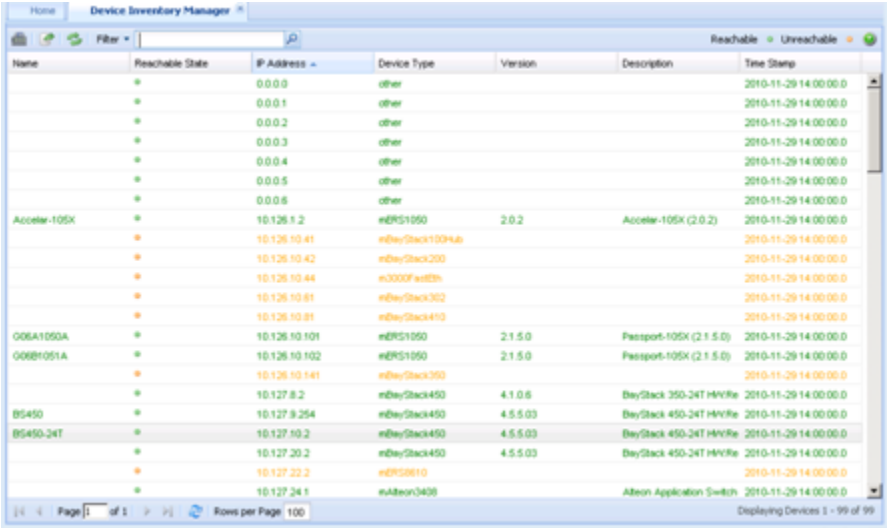


Figure 15: Device Inventory

The following figure shows the Device Manager toolbar.

Figure 16: Device Manager toolbar

The Device Inventory Manager allows you to

- launch Element Manager
- import or export inventory
- refresh

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

Chapter 7: Managers management

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. Asubmanager 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 following figures shows the Managers panel.

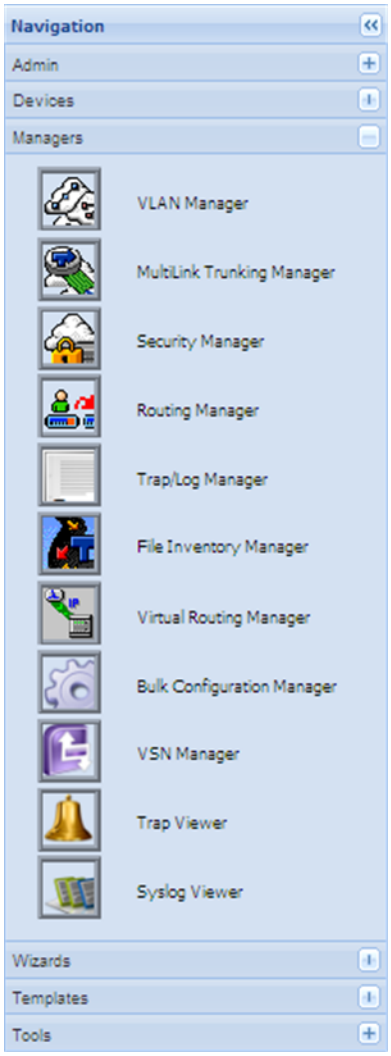


Figure 17: COM Managers

The submanagers are described in the following sections:

- VLAN Manager on page 73
- MultiLink Trunking Manager on page 73
- Security Manager on page 74
- Routing Manager on page 74
- Trap/Log Manager on page 75
- File Inventory Manager on page 75
- Virtual Routing Manager on page 76
- Bulk Configuration Manager on page 76
- VSN Manager on page 77

• Trap Viewer on page 77
• Syslog Viewer on page 77

VLAN Manager

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

VLAN Manager allows you to

- add, delete, modify and monitor VLANs 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 STGs
- view and edit port membership information for individual routing ports and bridge routing ports.
- view Spanning Tree configuration information in the COM topology map, such as the ports that are blocking or forwarding. User device is the root of the Spanning Tree configuration

For more information about Configuration of VLAN Manager, see *Avaya Configuration and Orchestration Manager Administration — Utilities* (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.

COM allows you to configure MultiLink Trunking across multiple devices:

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

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

Security Manager

Security Manager allows you to manage access to device and network management functions on network devices discovered by Configuration and Orchestration Manager. 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. Use security groups to group devices together that you want to have the same passwords and access features.

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

Routing Manager

Routing Manager allows you to 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 Configuration of Routing Manager, see *Avaya Configuration and Orchestration Manager Administration — Utilities* (NN47226-600).

Trap/Log Manager

The Trap/Log Manager is an Configuration and Orchestration Manager submanager that allows you to 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 of previous releases, and provides additional capabilities to configure traps, notifications, and syslogs.

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

File Inventory Manager

File Inventory Manager enables the user to manage the hardware and software configurations for different devices.

Use File Inventory Manager to upload and download image and configuration or boot files to and from devices and to back up, restore, archive, and synchronize image and configuration/boot files for those devices as well. In addition, File Inventory Manager allows you to

- view hardware configuration
- view software configuration
- edit Preferences
- download/Upload file from and to device
- backup/restore Configuration file
- archive Configuration file
- synchronize Configuration file
- upgrade Device
- compare runtime configuration with existing configuration

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

Virtual Routing Manager

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

To start Virtual Routing Manager

- The administrator user must assign the VRM to you in the MultiElementManager Assignment tab.
- The administrator must assign devices to you.

Virtual Routing Manager allows you to

- 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 configuration of Virtual Routing Manager, see *Avaya Configuration and Orchestration Manager Administration — Utilities* (NN47226-600).

Bulk Configuration Manager

You can launch the Bulk Configuration Manager (BCM) from the 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 the Bulk Configuration Manager, see *Avaya Bulk Configuration Manager Fundamentals*, and *Avaya Bulk Configuration Manager Installation*.

VSN Manager

The Virtual Services Network (VSN) Manager is a multielement manager that permits you to manage L2 Shortest Path Bridging MAC (SPBm) and L3 SPBms throughout the discovered network on ERS 8600 version 7.1 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 operations:

- 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—Utilities* (NN447226–600).

Trap Viewer

The Trap Viewer is a Configuration and Orchestration Manager (COM) tool that permits you to view Traps/ Notifications for devices. You can export information from the Trap Viewer to a text file; however, you cannot edit cells.

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

Syslog Viewer

The Syslog Viewer is a Configuration Orchestration Manager (COM) tool that permits you to 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—Utilities* (NN47226–600).

Chapter 8: Wizards management

The Avaya Configuration and Orchestration Manager (COM) wizards help you to configure complex network topologies and deployments using a small number of steps.

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

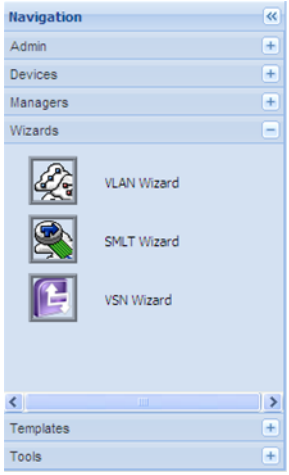


Figure 18: Wizards panel

There are three types of wizards:

- **VLAN Wizard**: VLAN Wizard allows you to configure STG and VLAN in multiple devices.

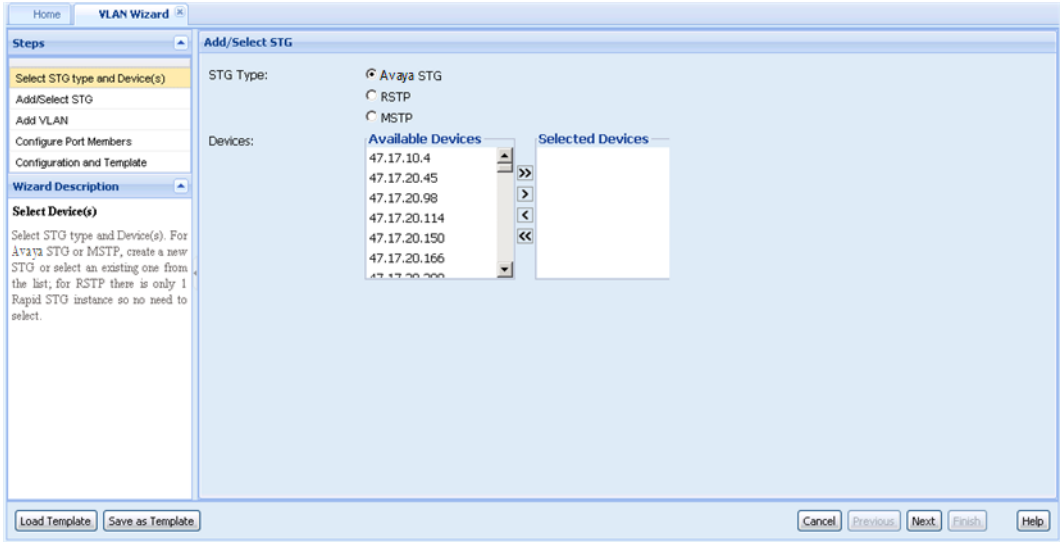


Figure 19: VLAN Wizard

- **SMLT Wizard**: SMLT Wizard guides the user into creating trunks configurations including necessary VLANs creation, various protocol enabling, and miscellaneous device settings.

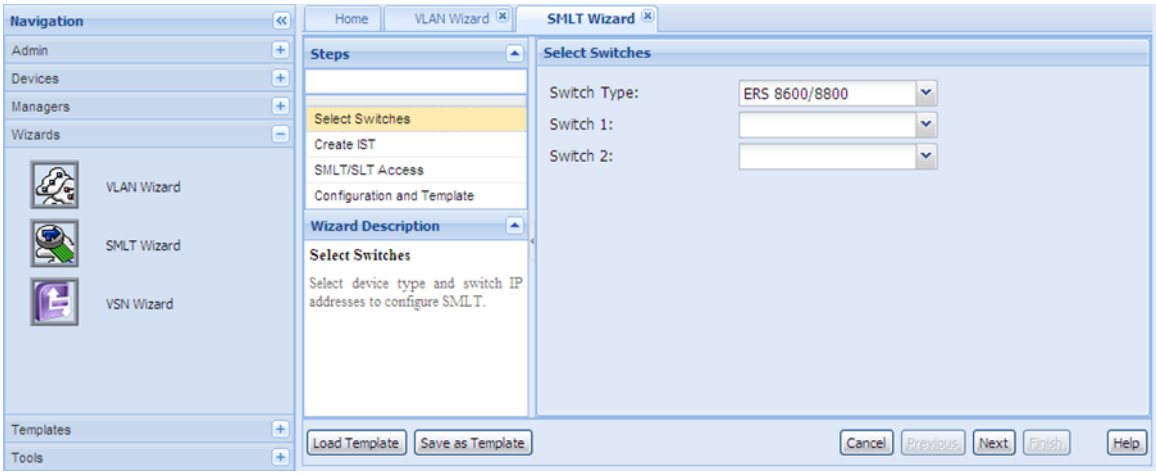


Figure 20: SMLT Wizard

- **VSN Wizard**: The Virtual Services Networks (VSN) wizard permits you to configure VSN service on multiple devices, and is composed of the following wizards:

  - SPB Infrastructure Wizard

  - L2 SPB Service Wizard

  - L3 SPB Service Wizard

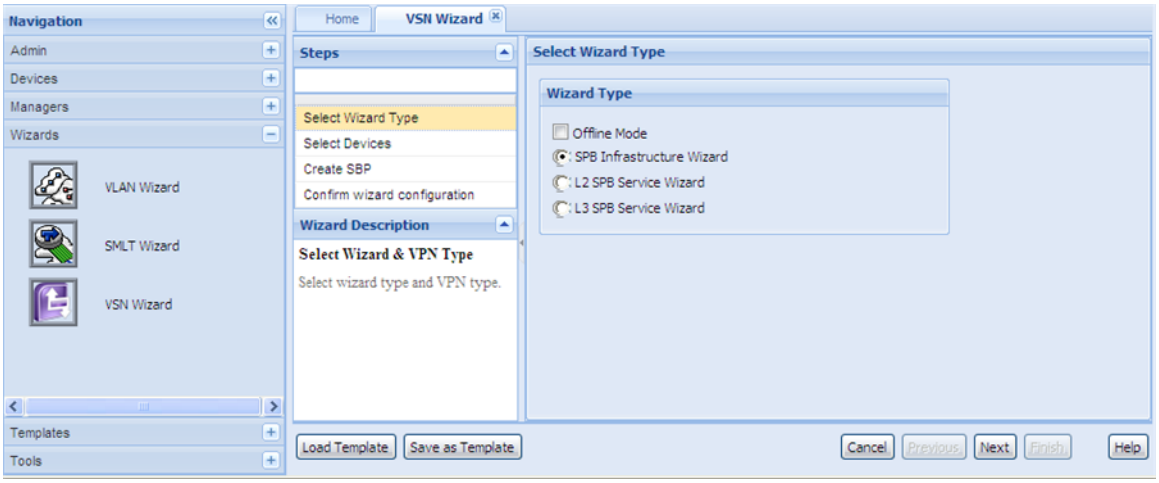


Figure 21: VSN Wizard

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

Chapter 9: Templates management

The template contains a set of configuration attributes. Templates can be created by running the Avaya Configuration and Orchestration Manager (COM) configuration wizards. At any point while running the wizard you can select to save the wizard configurations as a template. The saved templates can be viewed in the Templates dialog box and can be used later to easily perform the same or similar configurations.

In the Configuration and Orchestration Manager Navigation pane, click on the Templates button.

The following figure shows the templates dialog box.

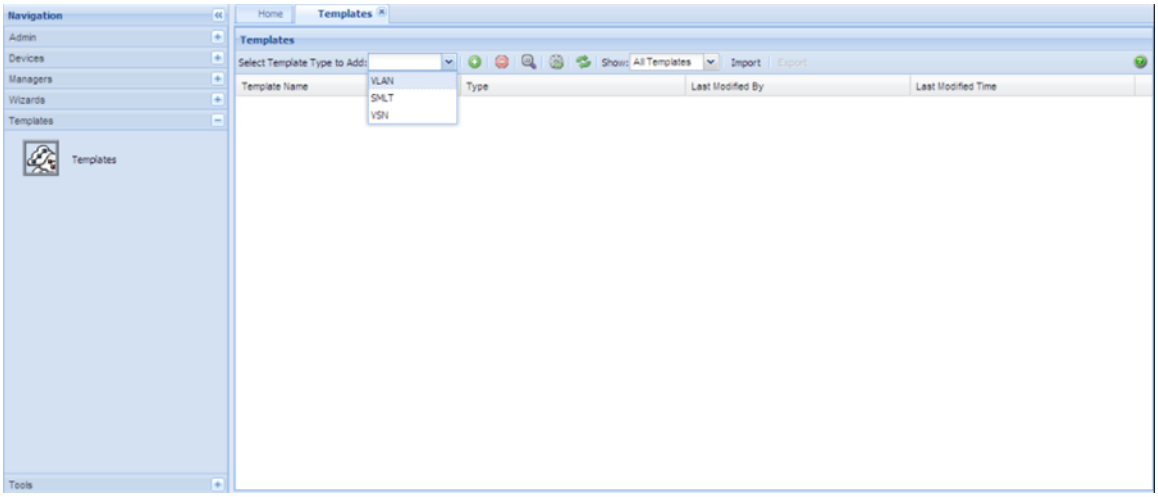


Figure 22: Templates dialog box

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. 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.

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

Chapter 10: Tools management

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. COM also provides a CLI manager and a Configuration Auditing Tool.

Navigation

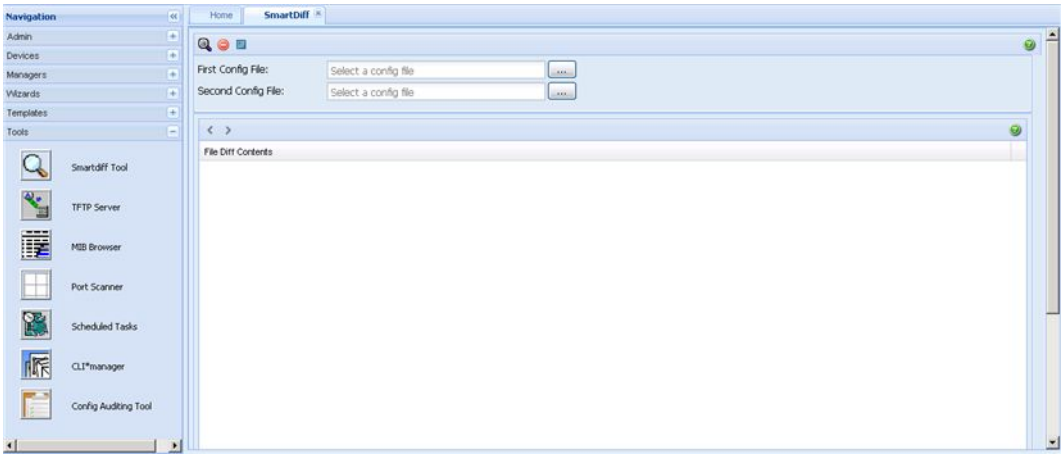
SmartDiff Tool

The SmartDiff tool allows you to compare two configuration file that have .cfg extension. Perform the following procedure to start the SmartDiff tool.

Procedure steps

In the Navigation pane, select the **Tools** panel, and then click the **SmartDiff Tool** icon.

The SmartDiff dialog box appears.



The following figure shows the SmartDiff toolbar.

Figure 23: SmartDiff toolbar

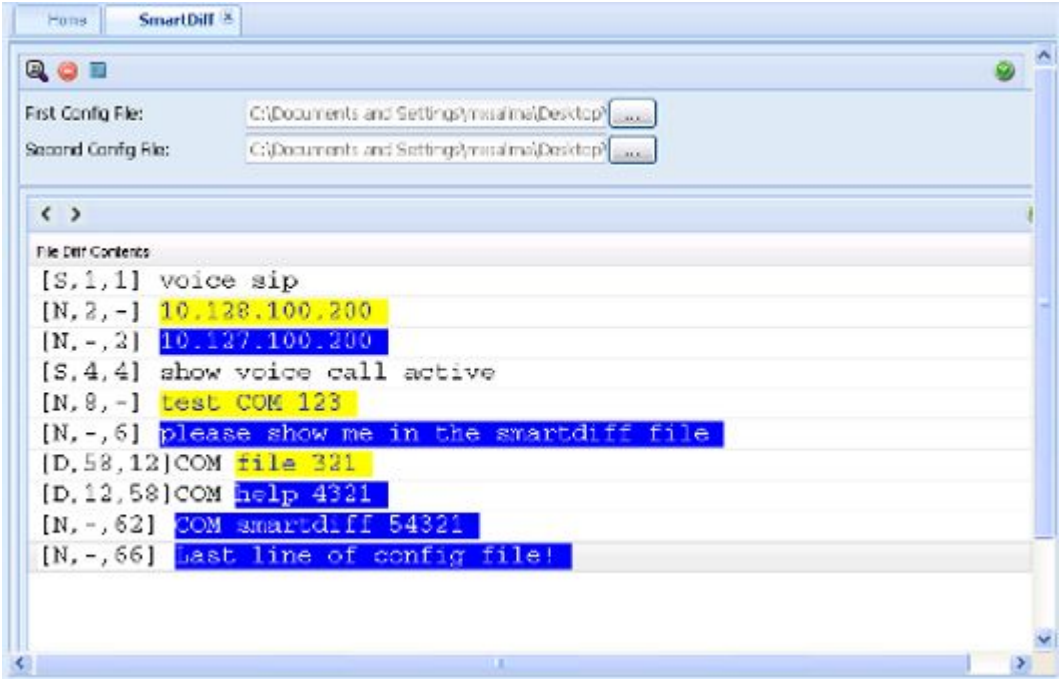
Comparing configuration files

Perform the following procedure to compare two configuration files.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click the **SmartDiff Tool** icon.
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.

   Click **Reset the input controls** to reset the **First Config File** and **Second Config File** fields value.
3. Click the **Show differences between files** icon from the toolbar. 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 white background indicates the matches text in a line.
- Blue Text in yellow background indicates any different text in the first line.
- White text in blue background indicates any different text in the second line
- Black text in grey background indicates the modified lines in the file.

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

TFTP Server

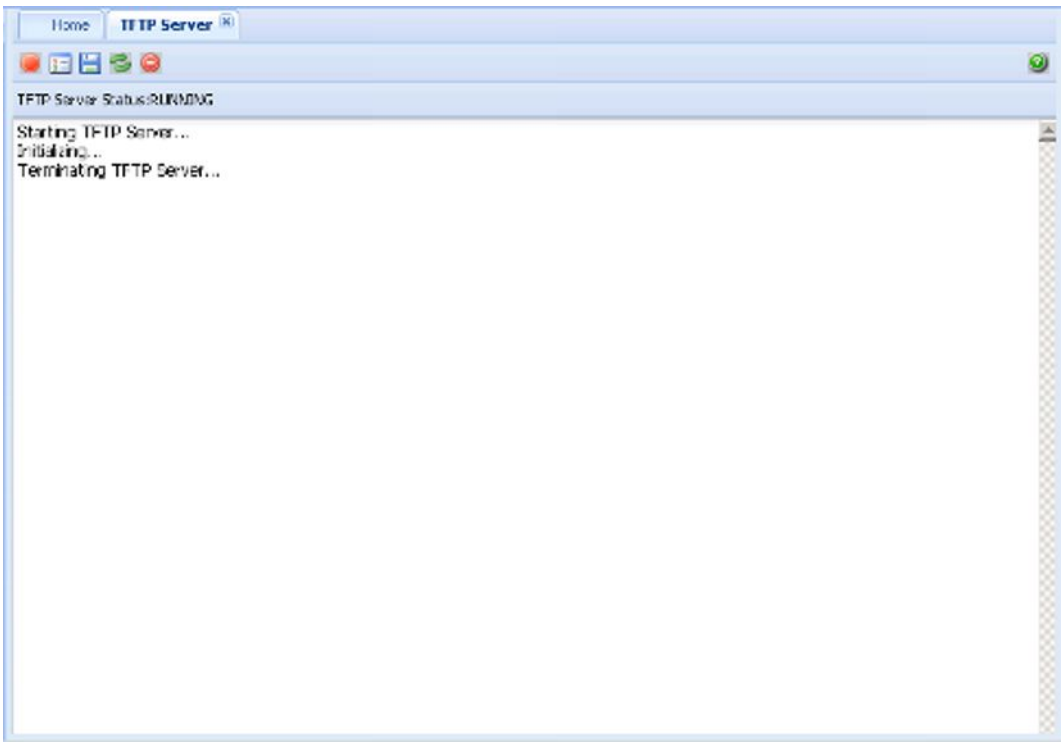
The TFTP Server tool allows you to view the status of TFTP server, start or stop TFTP server, and manage logs.

Perform the following procedure to view TFTP server.

Procedure steps

In the Navigation pane, select the **Tools** panel, and then click the **TFTP Server** icon.

The TFTP Server tab appears.



The following figure shows the TFTP Server toolbar.

Figure 24: TFTP Server toolbar

Navigation

- Viewing the status of TFTP Server on page 89
- Starting and stopping TFTP Server on page 89
- Editing preferences on page 90
- Saving log messages on page 91
- Refreshing log messages on page 91
- Clearing log messages on page 91

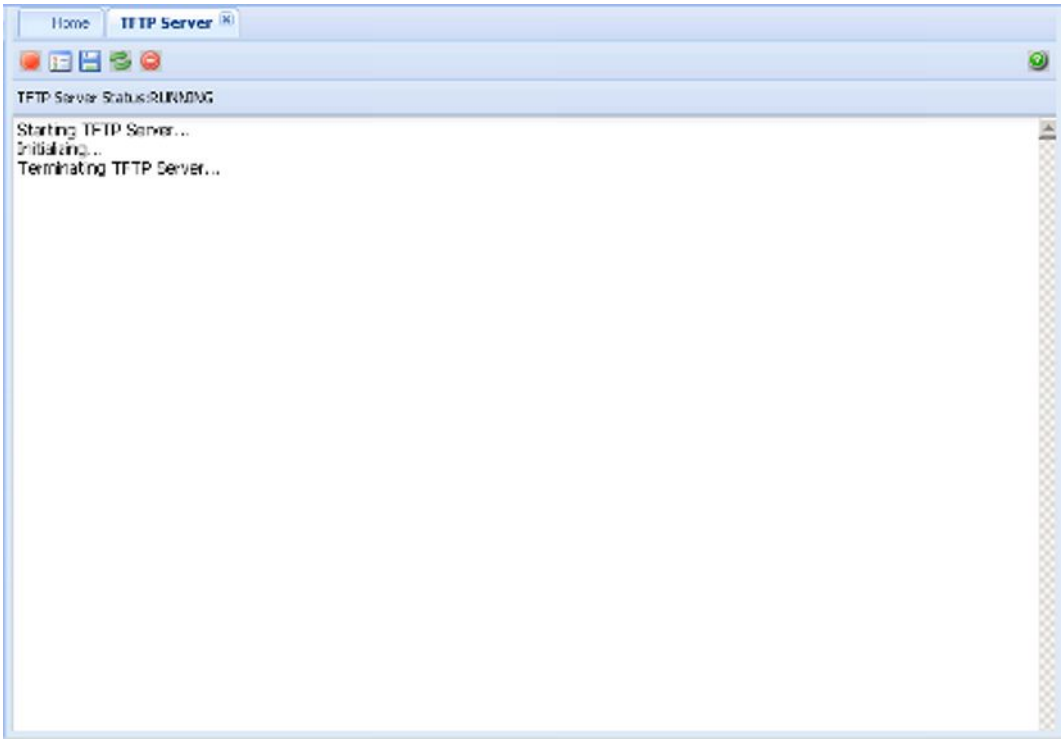
Viewing the status of TFTP Server

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

Procedure steps

In the Navigation pane, select the **Tools** panel, and then click the **TFTP Server** icon.

The TFTP Server tab appears showing the TFTP Server Status, as shown in the following figure.



Starting and stopping 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 the **TFTP Server** icon.

   The TFTP Server tab appears.

2. If the TFTP Server Status is running, click **Stop TFTP Server** from the toolbar to stop the TFTP Server. After stopping the TFTP Server, this button turns to **Start TFTP Server** . **OR** If the TFTP Server Status is stopped , click **Start TFTP Server**

from the toolbar to start the TFTP Server. After starting the TFTP Server, this button turns to **Stop TFTP Server** .

Editing preferences

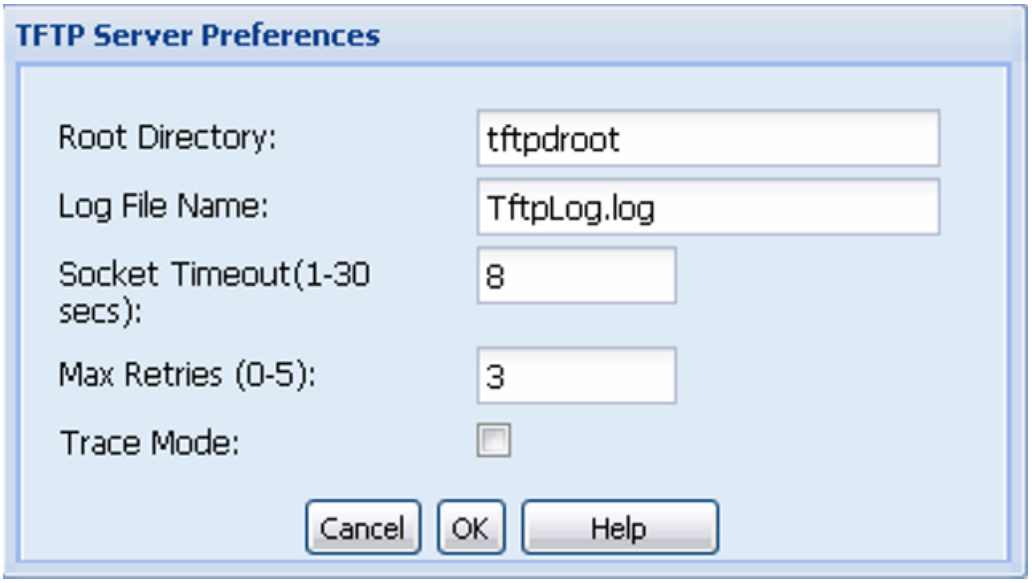
Perform the following procedure to edit TFTP Server preferences.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click the **TFTP Server** icon.

   The TFTP Server tab appears.

2. Click **Preferences** from the toolbar. The TFTP Server Preferences dialog box appears, as shown in the following figure.



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 TFTP Server Preference dialog box.

Table 7: TFTP Server Preferences table

Tab	Description
Root Directory	Specifies the root directory in the TFTP Server.
Log File Name	Specifies the log file name.

Tab	Description
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 the **TFTP Server** icon.

   The TFTP Server tab appears.
2. Click **Save Log Messages** from the toolbar 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 the **TFTP Server** icon.

   The TFTP Server tab appears.
2. Click **Refresh Log** from the toolbar 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 the **TFTP Server** icon.

   The TFTP Server tab appears.
2. Click **Clear Log Messages** from the toolbar. After you are prompted to confirm the clearing of log messages, click **Yes** to clear the current TFTP server log.

MIB Browser

MIB Browser allows you to 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 MIB Browser. MIB Browser also allows you to view and operate the data available through an SNMP agent in a managed device.

The following figure shows the MIB Browser tab.

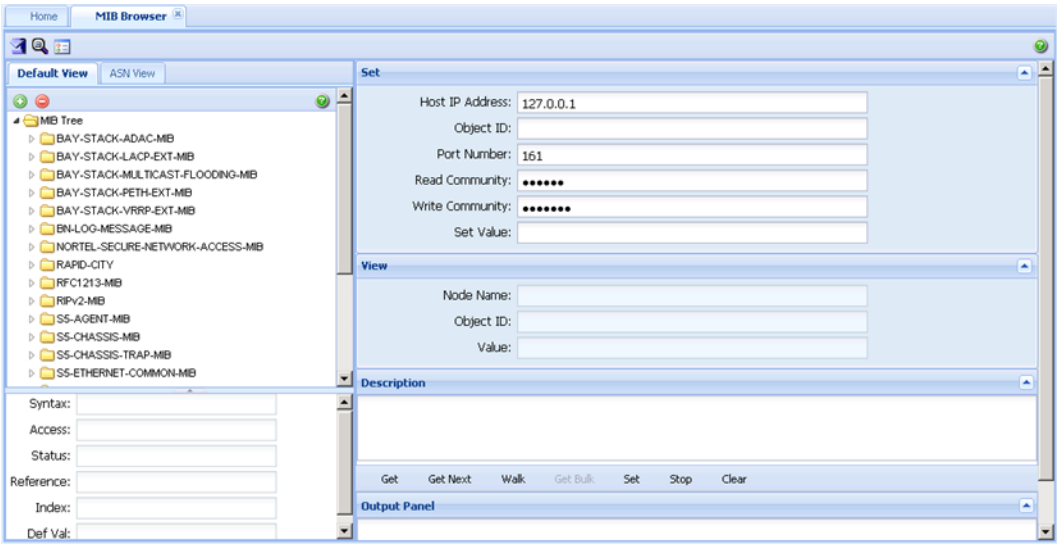


Figure 25: MIB Browser

The following table describes the parts of MIB Browser tab.

Table 8: Parts of MIB Browser tab

Part	Description
Views	Displays the currently loaded MIBs. Available views: Default view and ASN view; ASN view shows all MIBs in ASN format.
Set panel	Allows you 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 MIB Browser tab.

Table 9: MIB Browser tools

Tool	Icon	Description
Load MIB		Allows you to load an MIB.
Unload MIB		Allows you to unload an MIB.
Set SNMP Version		Allows you to set SNMP version. The available versions are as follows: • 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 93
- Unloading an MIB on page 94
- Setting SNMP version on page 94
- Retrieving data of an MIB node on page 96
- Traversing MIB tree on page 96
- Retrieving value of a subtree on page 96
- Retrieving data from a large table on page 97
- Editing data for MIB node on page 97

Loading an MIB

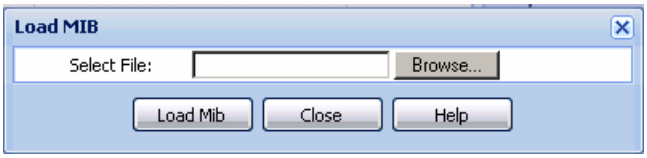
Perform the following procedure to load an MIB.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click the **MIB Browser** icon.

The MIB Browser tab appears.

2. Click the **Default View** or **ASN View** tab.
3. Click the **Load MIB** icon ((+) sign) from the toolbar. The Load MIB dialog box appears.



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 the **MIB Browser** icon.

   The MIB Browser tab appears.
2. Click the **Default view** tab and select the MIB node you want to delete.
3. Click the **Unload MIB** icon from the toolbar. After you are prompted to confirm the unloading.
4. Click **Yes** to unload the selected MIB. **OR** Click **No** to cancel the unload operation.

   The MIBs will be removed from the tree if you click Yes.

Setting SNMP version

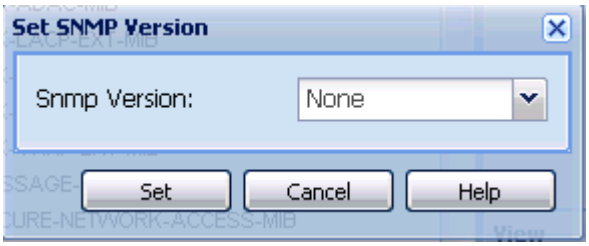
Perform the following procedure to set SNMP version of a MIB.

Procedure steps

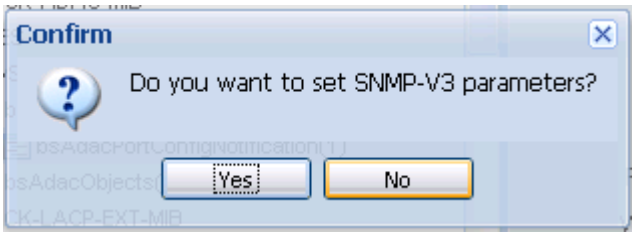
1. In the Navigation pane, select the **Tools** panel, and then click the **MIB Browser** icon.

The MIB Browser tab appears.

2. Click the **Default view** or **ASN View** tab and select an MIB which SNMP you wish to change.
3. Click the **Set SNMP Version** icon from the toolbar. The Set SNMP Version dialog box appears.



4. Choose the version that you wish to set in the **Snmp Version** field.
5. Click **Set**. After you are prompted to confirm the setting.



6. Click **Yes**. The SNMP V3 Settings dialog box appears, as shown in the following figure.

7. 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.
8. 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

1. In the Navigation pane, select the **Tools** panel, and then click the **MIB Browser** icon. The MIB Browser tab appears.
2. Select the desired node from the MIB tree.
3. Click **Get** from the menubar.

Traversing 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 the **MIB Browser** icon. The MIB Browser tab appears.
2. Select the desired node from the MIB tree.
3. Click **Get Next** from the menubar.

Retrieving value of a subtree

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

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click the **MIB Browser** icon. The MIB Browser tab appears.
2. Select the desired 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 the **MIB Browser** icon. The MIB Browser tab appears.
2. Select the desired 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 94.
4. Click **SNMP Bulk Setting** icon from the toolbar. The Get Bulk Panel appears.
5. Select a node from the MIB that you wish to add to the variable-bindings list, and then click **Add**.
6. Enter the value in **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 MIB node

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

Important:
The Set operation can be performed only on a node that has read-write access.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click the **MIB Browser** icon. The MIB Browser tab appears.
2. Select the desired node from the MIB tree.
3. Enter the value, you want to configure, in the **Set Value** field of **Set** panel.
4. Click **Set** from the menubar.

Job aid

The following table describes the fields of Get Bulk Panel.

Table 10: 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 SNMP-V3 Settings dialog box.

Table 11: SNMP-V3 Settings dialog box

Field	Description
User Name	Specifies the SNMPv3 user name.
Authentication	Specifies the Authentication protocol used.
Auth Password	Specifies password that is used for authentication purposes.
Privacy	Specifies the privacy protocol used.
Privacy Password	Specifies the password that is used for privacy purposes.

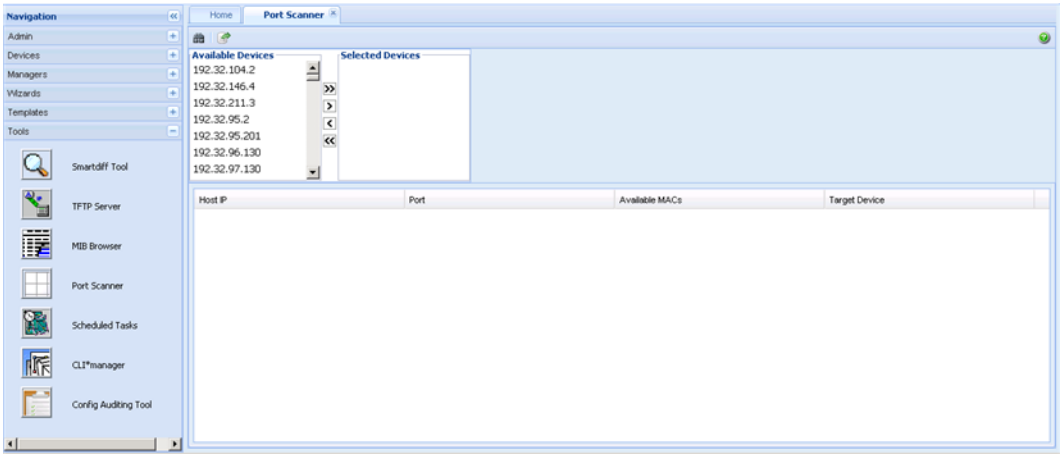
Port Scanner

Port Scanner allows you to 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

In the Navigation pane, select the **Tools** panel, and then click the **Port Scanner** icon.

The Port Scanner dialog box appears.



Navigation

- Scanning Ports on page 99
- Exporting report of port scan on page 99

Scanning Ports

Perform this procedure to scan ports of the selected device.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click the **Port Scanner** icon. The Port Scanner dialog box appears.
2. Select the devices, you wish to scan, in the **Available Device** field, and move to **Selected Devices** using **>** or **>>**.
3. Click the **Scan Ports** icon from the toolbar. The result is displayed in the content pane.

Exporting 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 the **Port Scanner** icon. The Port Scanner dialog box appears.
2. Select the devices, you wish to scan, in the **Available Device** field, and move to **Selected Devices** using **>** or **>>**.
3. Click the **Scan Ports** icon from the tool bar. The result is displayed in the content pane.
4. Click **Export** icon from the tool bar to export the report.

   The Export dialog box appears.
5. Select the type (html, or text) in **Export type** field, and then click **Ok**.

Job aid

The following table describes the parts of Port Scanner tab.

Table 12: Port Scanner tab

Part	Description
Toolbar	Provides you Scan Port and Export tools. • Scan Port—allows you to scan the target devices. • Export—allows you to export the result in text format.
Available Devices	Contains a list of assigned devices.
Selected Devices	Contains devices selected from Available Devices list.
>>	Allows you to move all the devices from the Available Devices list into the Selected Devices list.
>	Allows you to move the selected device from the Available Devices list into the Selected Devices list.
<	Allows you to move the selected device from the Selected Devices list to the Available Devices list.
<<	Allows you 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.

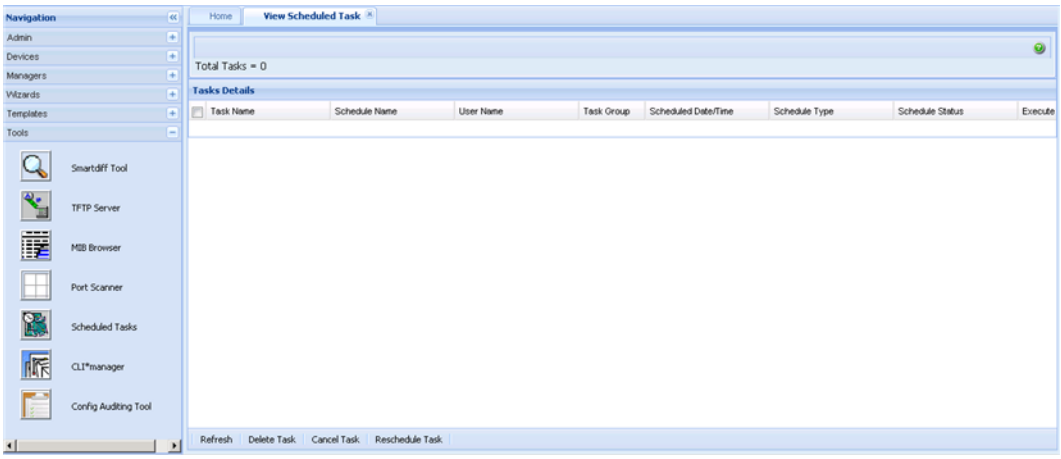
Scheduled Tasks

Using Sceduled Tasks tool, you can only view, delete, cancel or re-schedule tasks from the File Inventory Manager. Perform the following procedure to view the scheduled tasks.

Procedure steps

In the Navigation pane, select the **Tools** panel, and then click the **Scheduled Tasks** icon.

The Scheduled Tasks dialog box appears.



The following table describes the tools of Scheduled Tasks tab.

Table 13: 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.

Navigation

- Refreshing scheduled task list on page 102
- Deleting a scheduled task on page 102

- Canceling a scheduled task on page 102
- Rescheduling a scheduled task on page 102

Refreshing 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 the **Scheduled Tasks** icon. The View Scheduled Task tab appears listing all the scheduled tasks.
2. Click **Refresh** to refresh the list.

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 the **Scheduled Tasks** icon. The View Scheduled Task tab appears listing all the scheduled tasks.
2. Select the task that you wish to delete, and then click **Delete Task** to delete the selected 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 the **Scheduled Tasks** icon. The View Scheduled Task tab appears listing all the scheduled tasks.
2. Select the task that you wish to cancel, and then click **Cancel Task** to cancel the selected 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 the **Scheduled Tasks** icon. The View Scheduled Task tab appears listing all the scheduled tasks.
2. Select the task that you wish to reschedule, and then click **Reschedule Task** to reschedule the selected task.

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, logging, and so on.

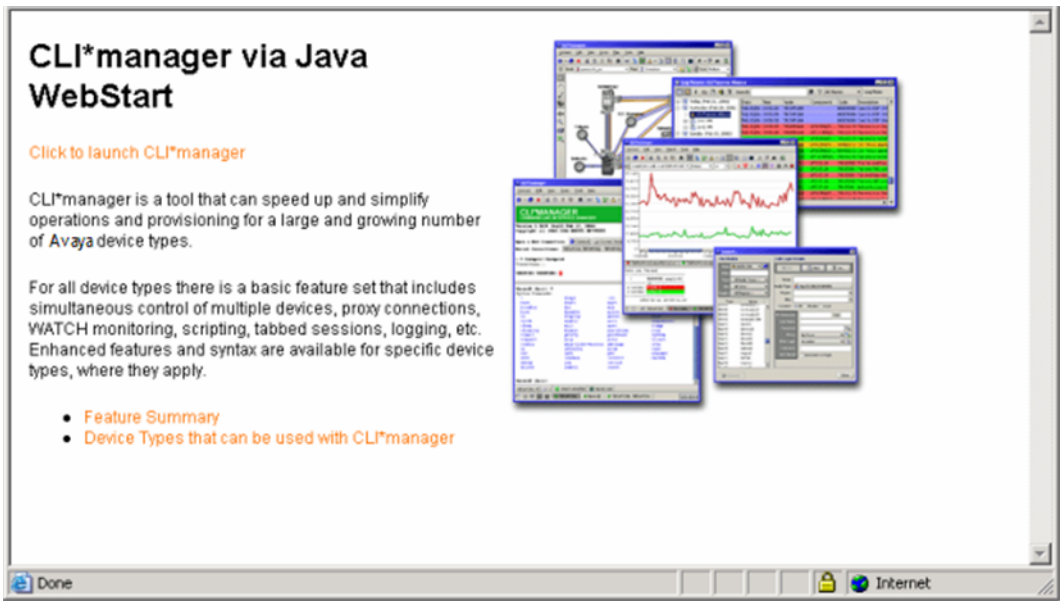
Prerequisites

You must install Java Virtual Machine (JVM).

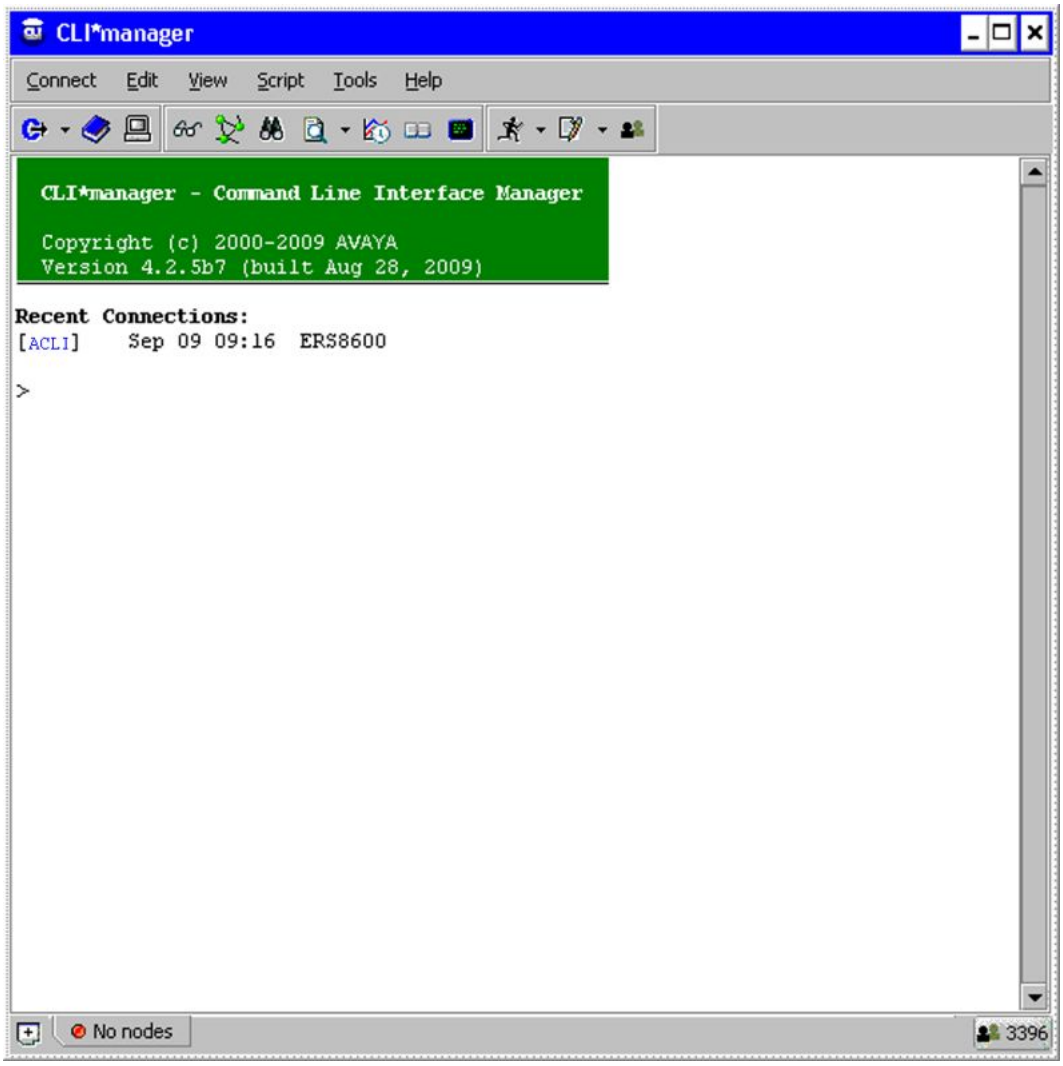
Perform the following procedure to launch the CLI*manager.

Procedure steps

1. In the Navigation pane, select the **Tools** panel, and then click the **CLI*manager** icon. The CLI*manager via Java WebStart page appears, as shown in the following figure.



2. Click the **Click to launch CLI*manager** link. The Warning - Security dialog box appears.
3. Click **Yes** to launch the CLI*manager.



Navigation

- CLI*manager user interface on page 106
- Connection set up on page 106
- Supported device type on page 107

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: Allows you to quickly switch between multiple active CLI sessions. Each tab shows the names of the active devices in its session, along with a small icon showing the current status of the session.
- 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. It also shows trees based on saved ASCII provisioning files.
- Flowcharts: Helps 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 by using standard up-and-down arrow keys, which opens a pop-up window for browsing to recent commands.
- Search: Finds specified text anywhere in its 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

Configuration Auditing Tool

The Configuration Auditing Tool allows you to 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 the **Config Auditing Tool** icon.

   The Configuration Auditing Tool opens in a separate window.
2. Click **Configuration Audit**.

   The Configuration Auditing Tool launches.
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 the **Export** button on the upper left of the panel and select **PDF**.

Table 14: Job aid

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

Chapter 11: Supported devices

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

Table 15: Device Requirements

Product family	Model	Versions
Belden L2E Switch	Hirschmann MICE-L2E	v.6.0.02
Belden L2P Switch	Hirschmann Railswitch –L2P	v.6.0.02
Belden L3P Switch	Hirschmann MACH-L3P	v.6.0.02
Avaya Ethernet Routing Switch 8600 series	8681XLW module	v.4.0, v.4.1, v.5.0, v.5.1, v.7.0, and v.7.1
	8681XLR module	
	8616GTE module	
	8672ATME MDA	
	8608GBM module	
	8608GTM module	
	8632TXM module	
	8648TXM module	
	8672ATMM module	
	8683POSM module	
Ethernet Routing Switch	8300 series	v.4.1.x and v.4.2
Ethernet Routing Switch	8800 series	all
Ethernet Routing Switch	5510, 5520 series	v.5.1, v.6.0, v.6.1, and v.6.2
Ethernet Routing Switch	56xx series	v.5.1, v.6.0, v.6.1, and v.6.2
Ethernet Routing Switch	5530 series	v.5.1, v.6.0 and v.6.1
Ethernet Routing Switch	45xx series	v.5.2, v.5.3, v.5.4, and v.5.5
Ethernet Routing Switch	25xx series	v.4.1.x , v.4.2, and v.4.3
Ethernet Routing Switch	16xx series	v.2.1.6.x and v.2.1.7.x
Virtual Services Platform	9000 series	v.3.0
Wireless Controller	8180	v.1.0
Wireless LAN AP	2220, 2221	v.1.3

Product family	Model	Versions
Wireless LAN AP	8120	v.1.0

Important:

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

Chapter 12: 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

There may be scenarios in which the COM installation server is in 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.
- It is recommended that the COM server chosen is as close as possible to the device, i.e. the lesser the hops to access the device the better.
- It is noted that the TFTP traffic typically does not pass through firewall and therefore TFTP server must run on subnets where devices are located.

Rediscoveries and device assignments

Network rediscoveries may result in 2 scenarios.

These scenarios can occur, while the changes in the network is not frequent. However, with device assignment function, the system administrator can assign users to devices depending on the requirement.

- Devices that are not discovered but exist in the assignment list — Devices are shown as invalid in the assignment list. System administrator understands that there is some fault

in the discovery or configuration and modifies the assignment list accordingly when device does not exist.

The invalid devices are shown in the following figure.

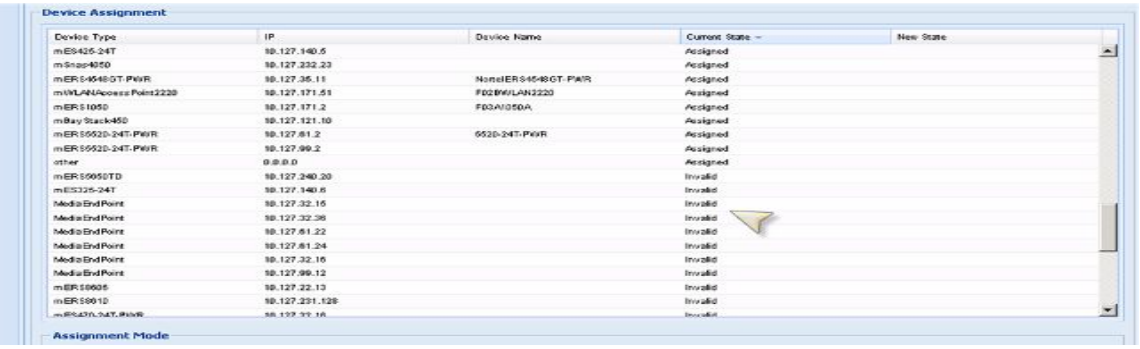


Figure 26: Invalid devices

- Devices that are newly discovered and now need to be assigned to some user — System administrator must assign the devices that are discovered to users who can access it.

  The unassigned devices are shown in the following figure.

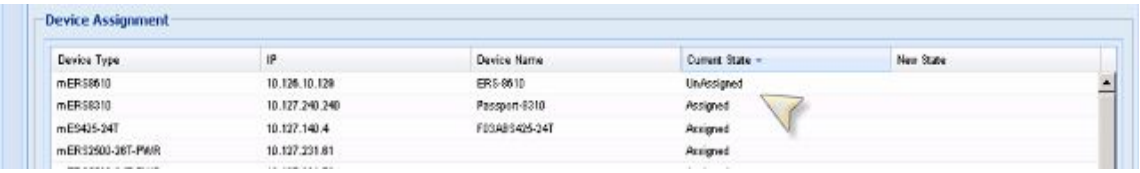


Figure 27: Unassigned devices

Internet browser Settings

Certain security settings in Internet Explorer (IE) does not allow Java script execution. In such a case, you can observe that the login page, does not show the login button. Following settings are recommended for IE.

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

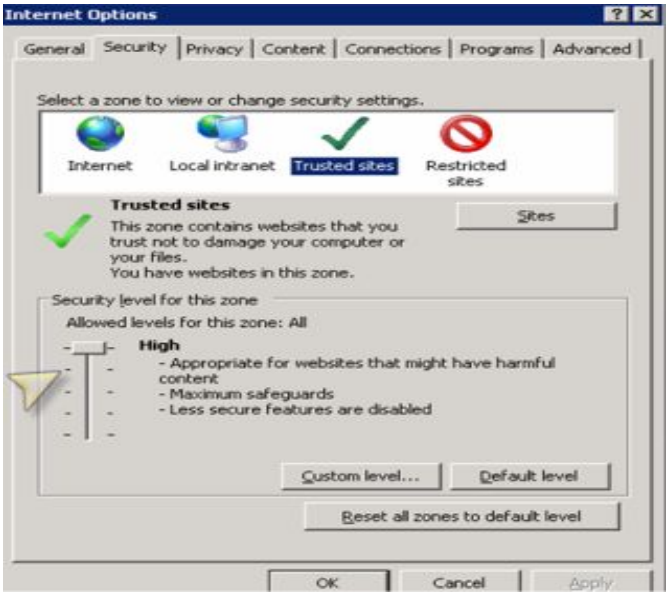


Figure 28: IE settings

- Additional settings for group policies that disable execution of scripts. It is recommended to try the same functionality in Firefox, in case if a problem persists.