



Nortel Configuration and Orchestration Manager

# Using the Product Interfaces

Document status: Standard  
Document version: 01.01  
Document date: 2 November 2009

Copyright © 2009, Nortel Networks  
All Rights Reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

### **Trademarks**

\*Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other products or services may be trademarks, registered trademarks, service marks, or registered service marks of their respective owners. The asterisk after a name denotes a trademarked item.

### **Restricted rights legend**

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

### **Statement of conditions**

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks reserves the right to make changes to the products described in this document without notice.

Nortel Networks does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

### **Nortel Networks software license agreement**

This Software License Agreement ("License Agreement") is between you, the end-user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. **Licensed Use of Software.** Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.
2. **Warranty.** Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.
3. **Limitation of Remedies.** IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The foregoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.
4. **General**
  - a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).
  - b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.
  - c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.
  - d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.
  - e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

- f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

---

# Contents

---

<b>New in this release</b>	<b>9</b>
Features	9
VLAN Manager	9
MultiLink Trunking Manager	9
Security Manager	10
Routing Manager	10
Trap/Log Manager	10
Virtual Routing and Forwarding Manager	10
Tools	10
<b>Introduction</b>	<b>11</b>
<b>Configuration and Orchestration Manager overview</b>	<b>13</b>
Introduction	13
Topology Manager	14
IEEE 802.1ab	14
Enabling discovery with 802.1ab	16
Navigation pane	17
Contents pane	19
Latest Logs pane	24
Links	25
<b>Configuration and Orchestration Manager logon</b>	<b>27</b>
Logging on to COM	27
<b>Configuration and Orchestration Manager administration</b>	<b>31</b>
Access Control	31
Assigning or unassigning devices	32
Resetting device assignments	33
Clearing device assignments	34
Removing invalid devices	35
Refreshing the device assignment list	36
Assigning MultiElement Manager	36
Resetting MultiElement Manager assignment	37
Clearing MultiElement Manager assignments	38
Refreshing the available multielement manager list	38

Preferences	39
Discovering devices	39
Configuring general system preferences	41
Configuring logging information	42
Device credentials	45
Adding a credential set	47
Adding a credential set for SNMPv3	48
Deleting a credential set	50
Editing a credential set	50
Importing a credential set	52
Exporting a credential set	53
User management	54
Viewing existing users	54
Adding a new local or external user	55
Disabling an user	58
Deleting a user	58
Licensing	59
Adding a license	59
Exporting a license	60
Generating a licensing report	61
Refreshing the license information	62
Plugins inventory	62
Downloading EDM plugin	63
Installing EDM plugin	63
Uninstalling EDM plugin	65
Refreshing the plugin inventory table	66
Selecting the EDM preferences	67
Audit log	68
Launching the audit log	68
Refreshing audit logs	69
<b>Devices management</b>	<b>71</b>
<b>Managers management</b>	<b>73</b>
VLAN Manager	74
MultiLink Trunking Manager	74
Security Manager	75
Routing Manager	75
Trap/Log Manager	76
File Inventory Manager	76
Virtual Routing Manager	77

---

<b>Wizards management</b>	<b>79</b>
<b>Templates management</b>	<b>81</b>
<b>Tools management</b>	<b>83</b>
SmartDiff Tool	83
Comparing configuration files	84
TFTP Server	85
Viewing the status of TFTP Server	87
Starting and stopping TFTP Server	87
Editing preferences	88
Saving log messages	89
Refreshing log messages	89
Clearing log messages	90
MIB Browser	90
Loading an MIB	92
Unloading an MIB	92
Setting SNMP version	93
Retrieving data of an MIB node	94
Traversing MIB tree	95
Retrieving value of a subtree	95
Retrieving data from a large table	96
Editing data for MIB node	96
Job aid	97
Job aid	97
Port Scanner	98
Navigation	98
Scanning Ports	98
Exporting report of port scan	99
Job aid	99
Scheduled Tasks	100
Refreshing scheduled task list	101
Deleting a scheduled task	101
Canceling a scheduled task	102
Rescheduling a scheduled task	102
CLI*manager	102
Navigation	104
CLI*manager user interface	105
Connection set up	105
Supported device type	106
<b>Appendix</b>	
<b>Recommendations and deployments</b>	<b>109</b>
COM installation server	109

---

## 8 Contents

---

Rediscoveries and device assignments	109
Internet browser Settings	110
License upgrades and device inventory	111



---

## New in this release

---

The following sections detail what's new in *Nortel Configuration and Orchestration Manager — Using the Product Interfaces* (NN47226-100) for Release COM 2.0.

### Features

See the following sections for information about feature changes.

- ["VLAN Manager" \(page 9\)](#)
- ["MultiLink Trunking Manager" \(page 9\)](#)
- ["Security Manager" \(page 10\)](#)
- ["Routing Manager" \(page 10\)](#)
- ["Trap/Log Manager" \(page 10\)](#)
- ["Virtual Routing and Forwarding Manager" \(page 10\)](#)
- ["Tools" \(page 10\)](#)

### VLAN Manager

Virtual Local Area Network (VLAN) Manager enables you to manage VLAN and STG configurations across a single device or multiple devices. It supports the rcVlan and rcStg. For more information about using the VLAN Manager, see *Nortel 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. MultiLink Trunking Manager manages MultiLink Trunks (MLTs) across devices in a network. You can also use MultiLink Trunking Manager to manage Split MultiLink Trunking (SMLT). For more information about using the MultiLink Trunking Manager, see *Nortel Configuration and Orchestration Manager Administration — Utilities* (NN47226-600).

### **Security Manager**

Security Manager allows you to manage access to device and network management functions on Ethernet Routing Switch 8000 series, Ethernet Routing Switch 55xx/35xx/45xx/25xx, Ethernet Switch, and Legacy BayStack devices discovered by Enterprise Switch Manager. For more information about using the Security Manager see, *Nortel Configuration and Orchestration Manager Administration — Utilities* (NN47226-600).

### **Routing Manager**

Routing Manager allows you to configure routing parameters for devices across a network. For more information about using the Routing Manager see *Nortel Configuration and Orchestration Manager Administration — Utilities* (NN47226-600).

### **Trap/Log Manager**

The Trap/Log Manager allows the user to fully manage trap and Syslog functionality on a managed network of Nortel Devices. For more information about using the Trap/Log Manager see, *Nortel Configuration and Orchestration Manager Administration — Utilities* (NN47226-600).

### **Virtual Routing and Forwarding Manager**

Virtual Routing and Forwarding Manager enables the user to manage Virtual Routing and Forwarding (VRF) configurations across specific devices. For more information about using the VRF Manager, see *Nortel Configuration and Orchestration Manager Administration — Utilities* (NN47226-600).

### **Tools**

In addition to the Managers, COM provides additional device and network management tools. For more information about Tools, see "[Tools management](#)" (page 83).

---

# Introduction

---

Configuration and Orchestration Manager (COM) provides you with an intuitive interface to configure, manage, and provision Nortel enterprise family of devices, such as Nortel Ethernet Routing Switches, Nortel 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

- ["Configuration and Orchestration Manager overview" \(page 13\)](#)
- ["Configuration and Orchestration Manager logon" \(page 27\)](#)
- ["Configuration and Orchestration Manager administration" \(page 31\)](#)
- ["Devices management" \(page 71\)](#)
- ["Managers management" \(page 73\)](#)
- ["Wizards management" \(page 79\)](#)
- ["Templates management" \(page 81\)](#)
- ["Tools management" \(page 83\)](#)



---

# Configuration and Orchestration Manager overview

---

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

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

## Navigation

- ["Introduction" \(page 13\)](#)
- ["Navigation pane" \(page 17\)](#)
- ["Contents pane" \(page 19\)](#)
- ["Latest Logs pane" \(page 24\)](#)
- ["Links" \(page 25\)](#)

## Introduction

COM provides you with an intuitive interface to configure, manage, and provision Nortel enterprise family of devices, such as Nortel Ethernet Routing Switches, Nortel 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 *Nortel 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 2.0 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 Nortel 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
- Nortel IP Phones

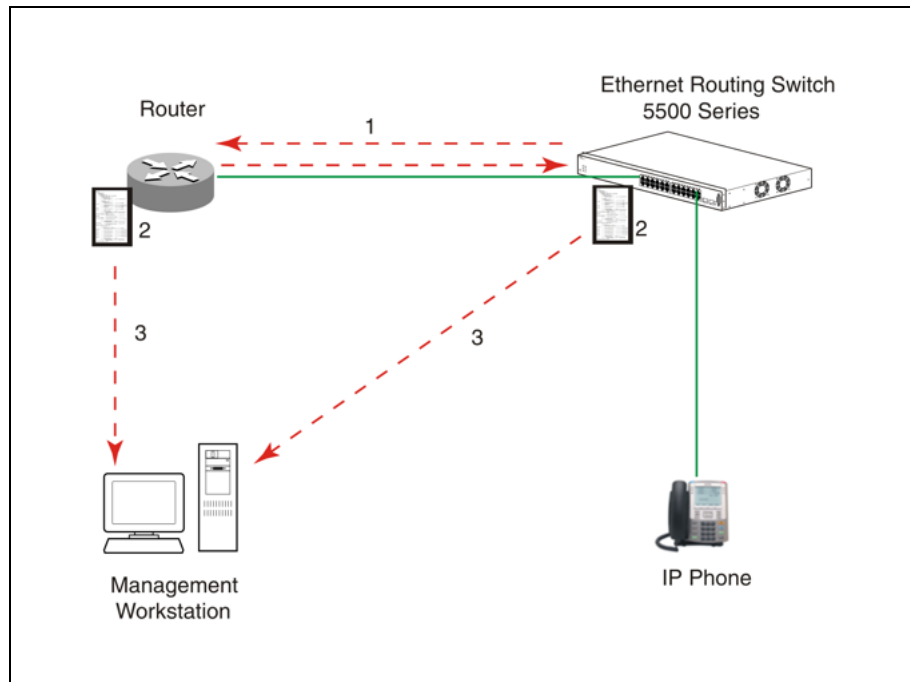
With 802.1ab support, Configuration Orchestration Manager is not restricted to the discovery of Nortel devices: it can discover any 802.1ab-enabled devices on the network, including third-party switches, routers, and IP Phones. Configuration Orchestration Manager can also display MED devices in the network.

#### **ATTENTION**

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 Nortel 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 " <a href="#">Navigation pane</a> " (page 17).
Contents pane	Displays a view of all the discovered devices and their relationship. For more information, see " <a href="#">Contents pane</a> " (page 19).
Latest Logs pane	Displays the last 15 traps and syslogs sent to COM from various devices. For more information, see " <a href="#">Latest Logs pane</a> " (page 24).
Links	Allows you to logout, access UCM home, COM details, and view Online Help. For more information, see " <a href="#">Links</a> " (page 25).

## Navigation pane

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

**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, and Virtual Routing Manager.
- **Wizards:** Contains VLAN and SMLT wizards.
- **Templates:** Contains the Template Manager.
- **Tools:** Contains SmartDiff Tool, TFTP Server, MIB Browser, Port Scanner, Scheduled Tasks, and CLI\*manager.

The Navigation pane displays the Contents pane.

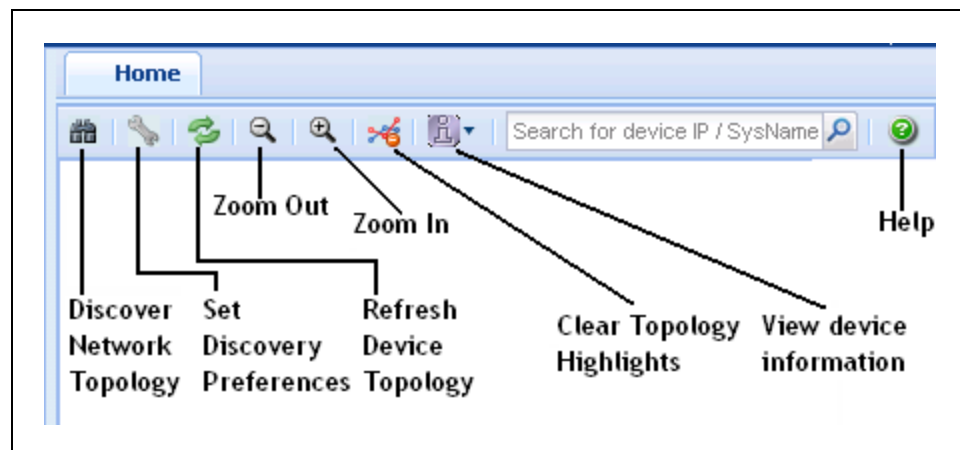
In the Navigation pane, click (+) to expand a panel and click (-) collapse a panel. You can click the (<<) to collapse the Navigation pane.

## Contents pane

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

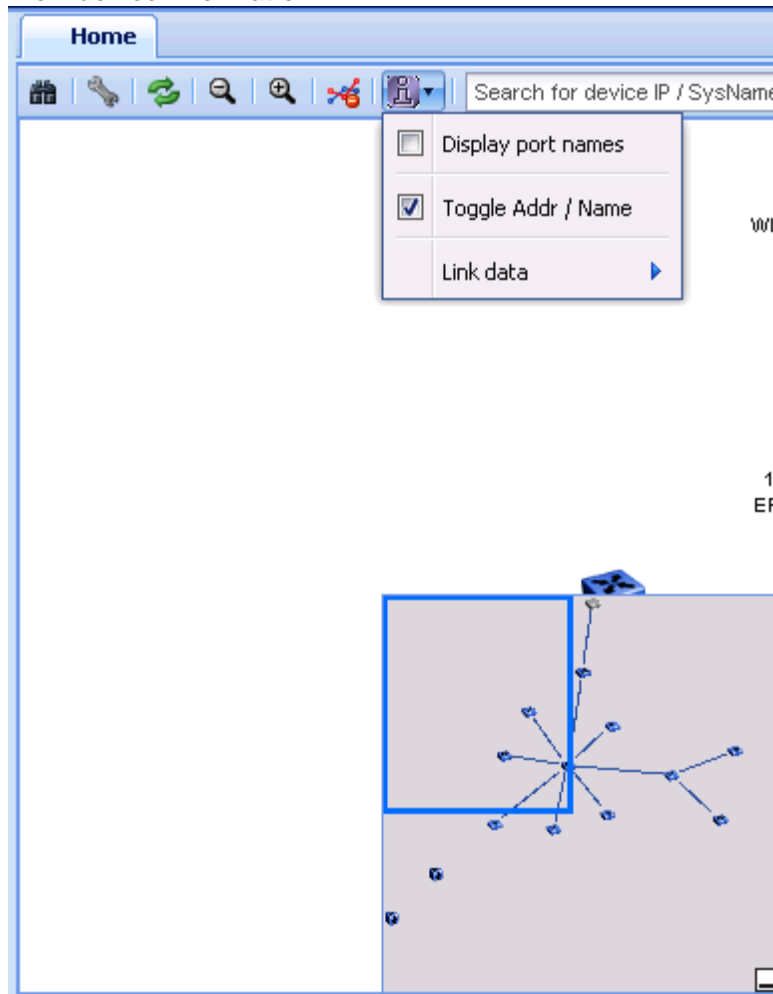
The following figure shows the buttons on the Contents pane.

**Figure 3**  
**Contents pane toolbar**



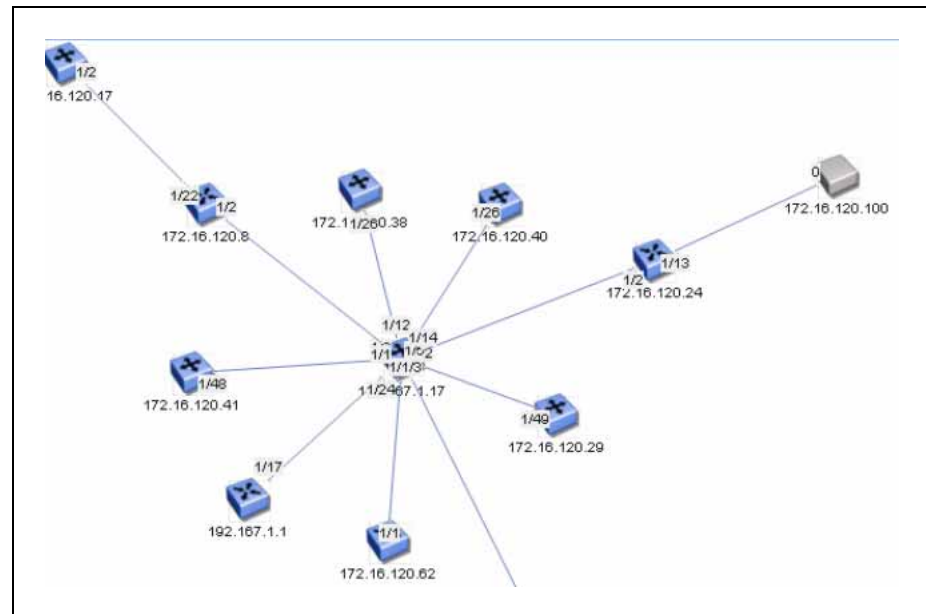
- **Discover Network Topology:** provides a view of all the discovered devices and their relationship.
- **Refresh Device Topology:** refreshes the topology view. It communicates with the server to get the latest discovered devices.
- **Zoom-in, Zoom-out Buttons:** allows you to zoom in or out the topology 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**



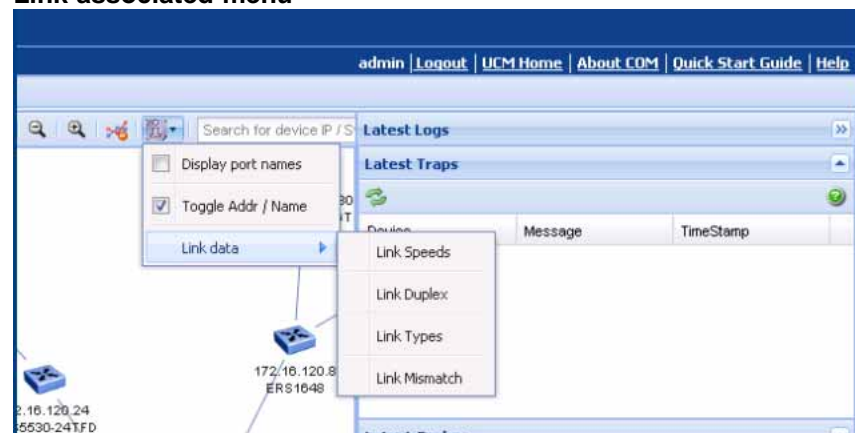
If a device in your topology has many links (port names or numbers) associated with it, then the topology map can be difficult to read. For example, in the following graphic, the seed IP address is 192.167.1.17; however, a port number (1/24) is overlapping the IP address making the IP address difficult 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**



- **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.

### ATTENTION

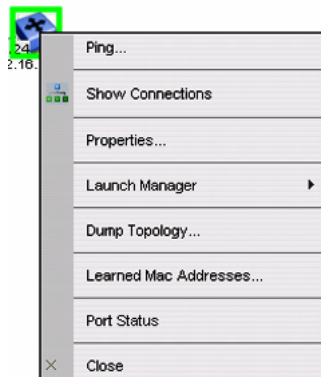
If the device is not found, then a Topology dialog box appears showing, "No additional matches found".

**Figure 7**  
**Search field**



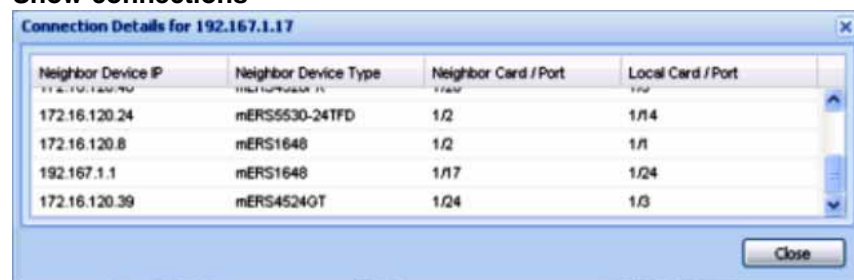
**Right-click menu:** displays a list of options available to you, when you right-click on the device.

**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.

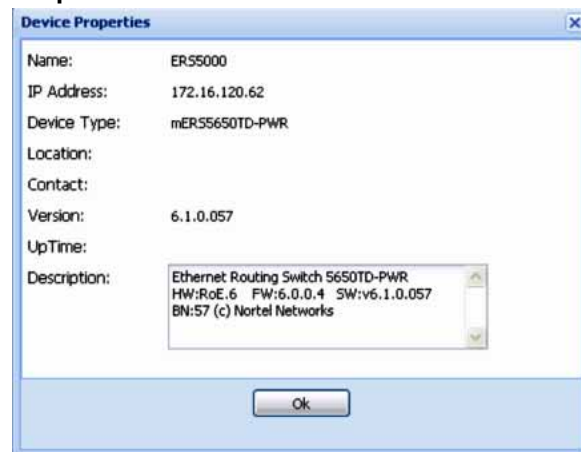
**Figure 9**  
**Show connections**



Neighbor Device IP	Neighbor Device Type	Neighbor Card / Port	Local Card / Port
172.16.120.24	mERS5530-24TFD	1/2	1/4
172.16.120.8	mERS1648	1/2	1/1
192.167.1.1	mERS1648	1/17	1/24
172.16.120.39	mERS4524GT	1/24	1/3

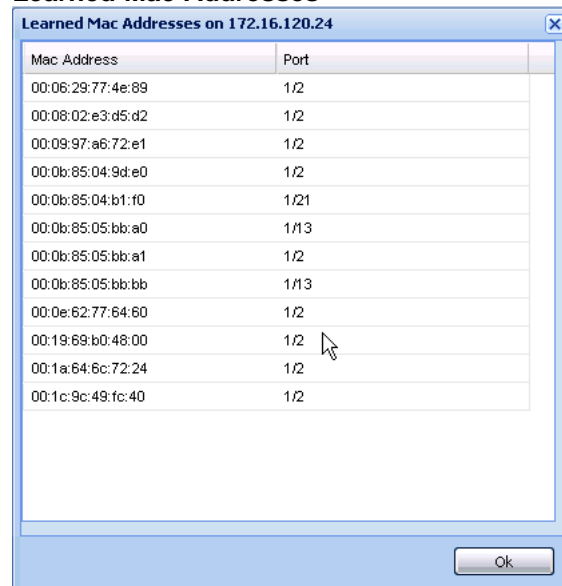
- **Properties:** displays properties of the device.

**Figure 10**  
**Properties**



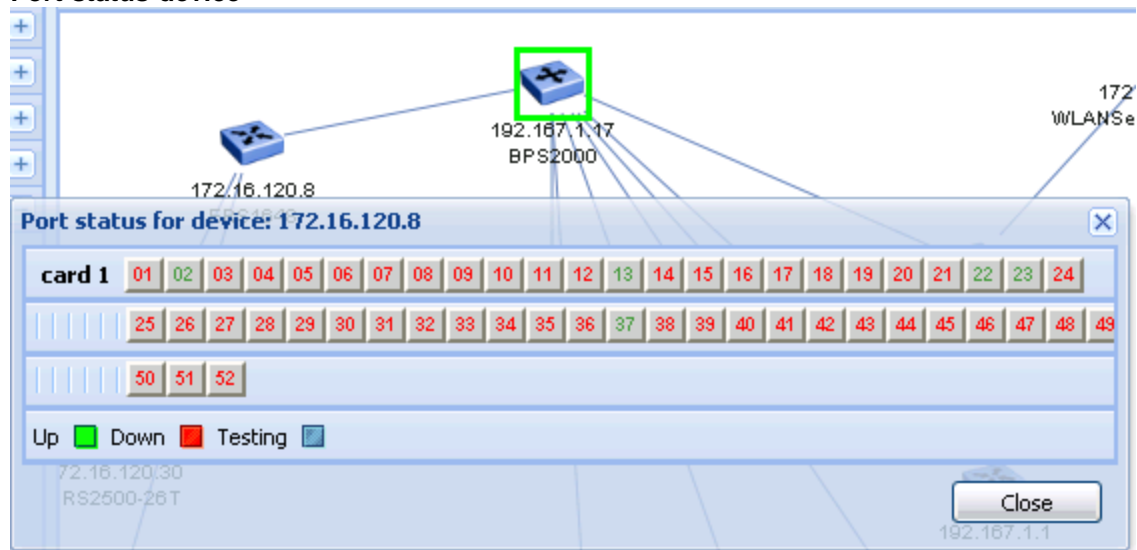
- **Launch Manager:** launches the element manager for the selected device.
- **Dump Topology:** displays the topology based on the real-time queries of devices.
- **Learned Mac Addresses:** displays the learned Mac addresses on the selected device.

**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 Latest Traps and Syslogs. It displays the last 15 traps and syslogs sent to COM from various devices. A refresh button is available in the Latest Traps and Latest Syslogs panel that always requests the last 15 logs from the server. You can collapse the Latest Logs pane to maximize the topology area.

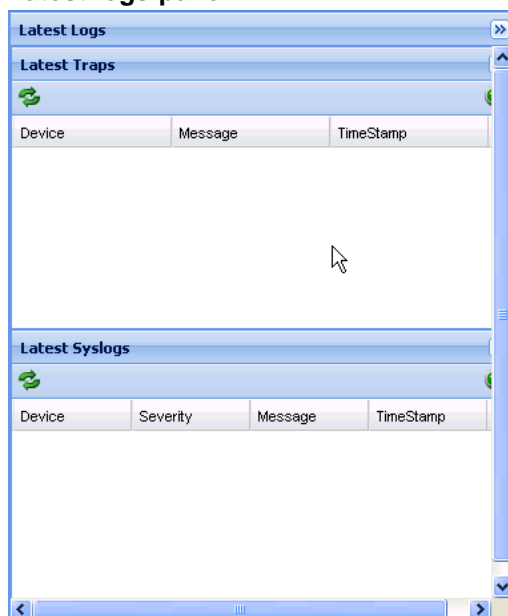
When you open a new tab, then all the existing tabs (topology and latest logs) become inactive.

The Latest Logs pane contains the following panels:

- **Latest Traps:** lists the latest traps for a device. A message and timestamp is provided for each device trap.
- **Latest Syslogs:** lists the latest syslogs for a device. Severity level, message, and timestamp are provided for each device syslog.



**Figure 13**  
**Latest logs pane**



## Links

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

- **admin:** shows the current logged in user name.
- **Logout:** logs you off from the Unified Communication 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.
- **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**



---

# Configuration and Orchestration Manager logon

---

This section describes how to start and log on to Configuration and Orchestration Manager (COM). For more information about how to install Configuration and Orchestration Manager, see *Configuration and Orchestration Manager — Installation* (NN47226-300).

## Logging on to COM

Perform the following procedure to start the COM application.

### Prerequisites

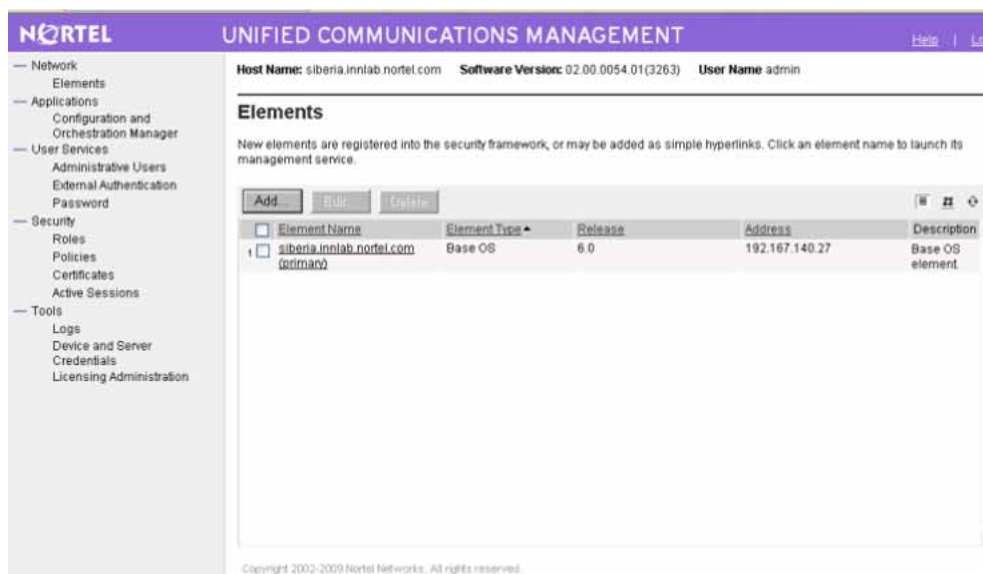
- You must install COM.
- You require Internet Explorer 7, or Firefox 3.0 if logging on with a client PC.

### Procedure steps

Step	Action
1	Start a Web browser supported by COM.
2	In the <b>Address</b> field, enter the Fully Qualified Device Name (FQDN) of the COM server.  The COM logon screen appears.

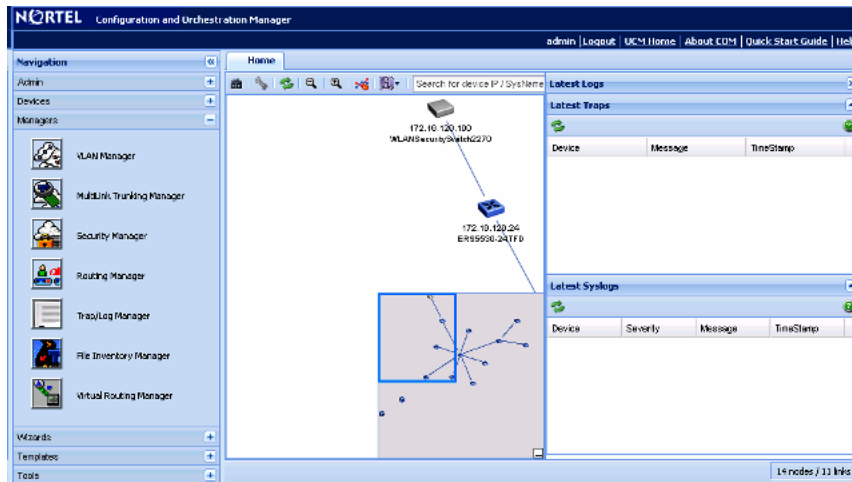


- 3 In the **User ID** field, enter the installed COM user ID.  
The default user ID is **admin**.
- 4 In the **Password** field, enter the installed COM password.
- 5 Click **Log In**.  
The Unified Communications Management (UCM) home page appears.



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

The COM home page appears.



---

—End—

---



---

# Configuration and Orchestration Manager administration

---

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

## Navigation

- "Access Control" (page 31)
- "Preferences" (page 39)
- "Device credentials" (page 45)
- "User management" (page 54)
- "Licensing" (page 59)
- "Plugins inventory" (page 62)
- "Audit log" (page 68)

## 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.

### **ATTENTION**

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" (page 32)
- "Resetting device assignments" (page 33)
- "Clearing device assignments" (page 34)
- "Removing invalid devices" (page 35)
- "Refreshing the device assignment list" (page 36)
- "Assigning MultiElement Manager" (page 36)
- "Resetting MultiElement Manager assignment" (page 37)
- "Clearing MultiElement Manager assignments" (page 38)
- "Refreshing the available multielement manager list" (page 38)

### 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

---

Step	Action
------	--------

---

- |   |  |
|---|--|
| 1 | From the Navigation pane, expand the <b>Admin</b> pane, and then click <b>Access Control</b> . |
|---|--|

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



Home Access Control

Device Assignment MultiElementManager Assignment

Select User: admin

Device Assignment

Device Type	IP	Device Name	Current State	New State
mERS5530-24TFD	172.16.120.24	5530-24TFD	Assigned	
mERS4524GT	172.16.120.39		Assigned	
mWLANSecuritySwitch2270	172.16.120.100		Assigned	
mERS8610	172.16.120.2	ERS-8610	Assigned	
mERS4526T	172.16.120.38	4526	Assigned	
mERS650TD-PWR	172.16.120.62	ERS5000	Assigned	
mERS8606	172.16.120.5	ERS-8606	Assigned	
mERS2500-26T	172.16.120.30		Assigned	

Assignment Mode

Assign/UnAssign: Selected Row Assign UnAssign Select All (Total 14 devices)

Apply Reset Clear User Assignments Remove Invalid Devices

- 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.

---

—End—

---

### 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

---

Step	Action
1	From the Navigation pane, expand the <b>Admin</b> pane, and then click <b>Access Control</b> .  The Access Control tab appears (in the Contents pane) with the Device Assignment tab selected.
2	From the <b>Select User</b> list, select the user.
3	From the <b>Device Assignment</b> table, select the device names that you want to reset.
4	Click <b>Reset</b> .

---

—End—

---

### Clearing device assignments

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

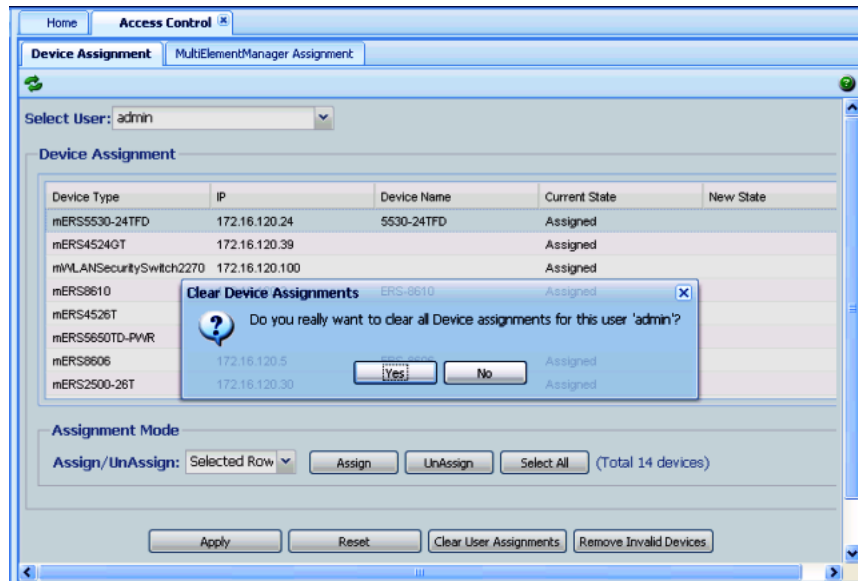
#### Prerequisites

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

### Procedure steps

---

Step	Action
1	From the Navigation pane, expand the <b>Admin</b> pane, and then click <b>Access Control</b> .  The Access Control tab appears (in the Contents pane) with the Device Assignment tab selected.
2	From the <b>Select User</b> list, select the user.
3	Click <b>Clear User Assignments</b> .  The Clear Device Assignments dialog box appears.



- 4 Click **Yes**.

—End—

## 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

Step	Action
------	--------

- |   |  |
|---|--|
| 1 | From the Navigation pane, expand the <b>Admin</b> pane, and then click <b>Access Control</b> .<br><br>The Access Control tab appears (in the Contents pane) with the Device Assignment tab selected. |
| 2 | From the <b>Select User</b> list, select the user.   |
| 3 | Click <b>Remove Invalid Devices</b> .<br><br>All the invalid devices in the COM server are removed.  |
| 4 | Click <b>OK</b> .  |

---

—End—

---

### 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

Step	Action
1	From the Navigation pane, expand the <b>Admin</b> pane, and then click <b>Access Control</b> .  The Access Control tab appears (in the Contents pane) with the Device Assignment tab selected.
2	From the <b>Select User</b> list, select the user.
3	Click <b>Refresh</b> .

---

—End—

---

### Assigning MultiElement Manager

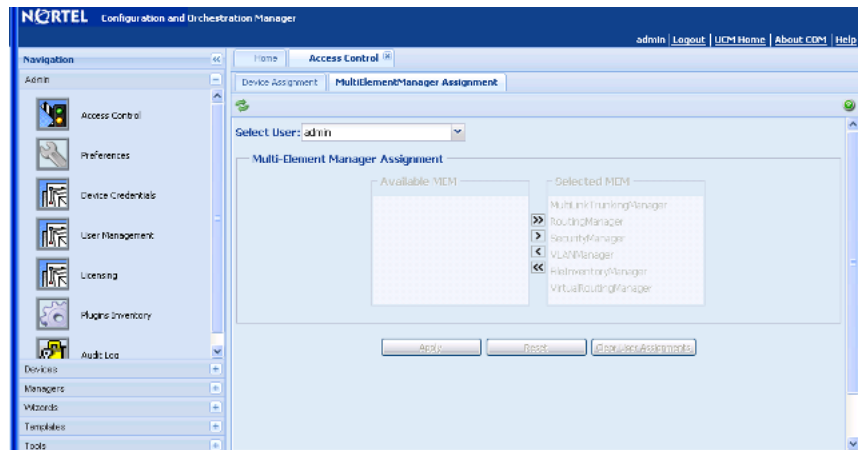
Perform the following procedure to assign the MultiElement Manager to the selected COM user.

#### Prerequisites

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

#### Procedure Steps

Step	Action
1	From the Navigation pane, expand the <b>Admin</b> pane, and then click <b>Access Control</b> .  The Access Control tab appears (in the Contents pane) with the Device Assignment tab selected.
2	Click the <b>MultiElementManager Assignment</b> 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 managers, 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**.

---

—End—

---

### 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

Step	Action
1	From the Navigation pane, expand the <b>Admin</b> pane, and then click <b>Access Control</b> .  The Access Control tab appears (in the Contents pane) with the Device Assignment tab selected.
2	Click the <b>MultiElementManager Assignment</b> tab.
3	From the <b>Select User</b> list, select the user.
4	Click <b>Reset</b> .

---

—End—

---

### 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

Step	Action
1	From the Navigation pane, expand the <b>Admin</b> pane, and then click <b>Access Control</b> .  The Access Control tab appears (in the Contents pane) with the Device Assignment tab selected.
2	Click the <b>MultiElementManager Assignment</b> tab.
3	From the <b>Select User</b> list, select the user.
4	Click <b>Clear User Assignments</b> .

---

—End—

---

### 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**

Step	Action
1	From the Navigation pane, expand the <b>Admin</b> pane, and then click <b>Access Control</b> .  The Access Control tab appears (in the Contents pane) with the Device Assignment tab selected.
2	Click the <b>MultiElementManager Assignment</b> tab.
3	From the <b>Select User</b> list, select the user.
4	Click <b>Refresh</b> .

---

—End—

---

**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.

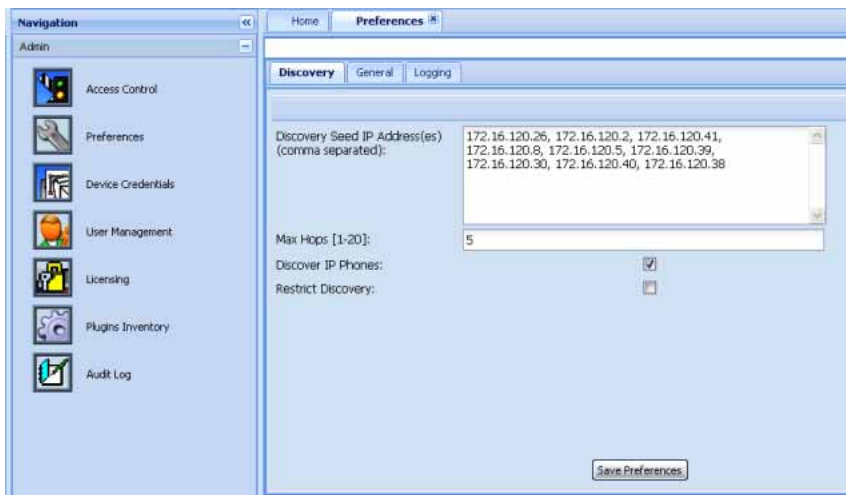
- ["Discovering devices" \(page 39\)](#)
- ["Configuring general system preferences" \(page 41\)](#)
- ["Configuring logging information" \(page 42\)](#)

**Discovering devices**

Perform the following procedure to discover devices for COM.

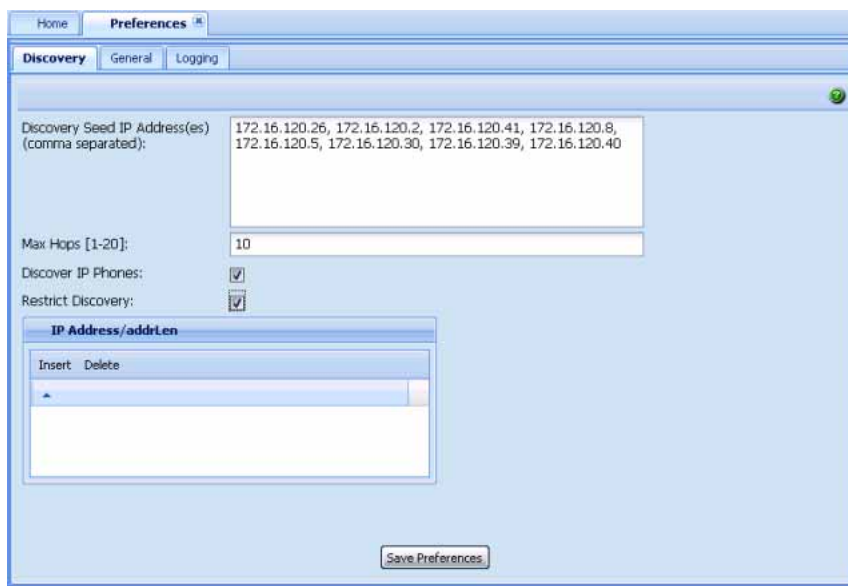
**Procedure steps**

Step	Action
1	From the Navigation pane, open <b>Admin</b> and then select <b>Preferences</b> .  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 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.





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

---

—End—

---

## Configuring general system preferences

Perform the following procedure to configure the general system preferences.

### Procedure steps

Step	Action
------	--------

- 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.

The screenshot shows the 'Preferences' dialog box with the 'General' tab selected. The 'SNMP' section contains the following settings: Retry Count (1), Timeout (5), Max Outstanding Requests (100), Listen for Traps (checked), Listen for Syslogs (checked), Trap Listener Port (162), and System Log Listener Port (514). The 'Database Clean-up' section contains: Trap/Syslog Storage (90 days), Trap/Syslog Check Time (1 hour), and Trap/Syslog Check (0). A 'Save Preferences' button is located at the bottom right of the dialog.

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

---

—End—

---

### Configuring logging information

Perform the following procedure to configure logging.

#### Procedure steps

---

Step	Action
------	--------

---

- |   |  |
|---|--|
| 1 | From the Navigation pane, open <b>Admin</b> and then select <b>Preferences</b> .<br>The Preferences dialog box appears in the Contents pane. |
| 2 | Click <b>Logging</b> .<br>The Logging dialog box appears.  |

Home Preferences

Discovery General **Logging**

Debug Log File Size[Example, 10 KB 10 MB 10 GB]: 10 MB

Audit Log File Size[Example, 10 KB 10 MB 10 GB]: 10 MB

Debug Log Level: ALL

Audit Log Level: INFO

Trace:

Debug Log No Files[1-10]: 3

Audit Log No Files[1-10]: 3

Save Preferences

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

---

—End—

---

### Job aid

The following table describes the fields of Preference tabs.

## Preferences fields

Tab	Item	Description
Discovery	Seed Address(es)	<p>The IP addresses of one or more devices that COM queries using SNMP to start the discovery process. For more information about supported devices, see <i>Nortel Configuration and Orchestration Manager Administration — Utilities</i> (NN47226-600).</p> <div style="border: 1px solid black; padding: 5px; text-align: center;"> <p><b>ATTENTION</b></p> <p>If the devices you want to monitor and configure are not connected to the same network, you can specify multiple seed addresses, separated by commas. Separate networks do not appear to be connected in the network topology map.</p> </div>
	Max Hops	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	SNMPRetry Count	The number of times, between 0 and 5, COM tries to connect to a device using SNMP. The default value is 1.
	Timeout	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	The number of SNMP requests, between 20 and 250, that COM maintains as open or outstanding. The default value is 100.
	Listen for Traps	If checked, COM receives traps for all the devices managed through COM.
	Listen for Syslogs	If checked, COM receives logs for all the devices managed through COM.

Tab		
Database Clean-up	Trap/Syslog Storage (days)	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 Checktime (Hour)	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 Checktime (Min)	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 Checktime Frequency (days)	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.
TFTP	TFTP Server	Allows you to enter the IP address of the default TFTP server used by submanager applications.
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	<p>If checked, additional SNMP information is written to COM error log, and can provide assistance in troubleshooting.</p> <div style="border: 1px solid black; padding: 10px; text-align: center;"> <p><b>ATTENTION</b></p> <p>Selecting Trace can slightly slow down performance as extra information is gathered</p> </div>
	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

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

**Table 2**  
**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
Windows Server	Windows User name Windows Password Windows Domain

## Navigation

- ["Adding a credential set" \(page 47\)](#)

- "Deleting a credential set" (page 50)
- "Editing a credential set" (page 50)
- "Importing a credential set" (page 52)
- "Exporting a credential set" (page 53)

### Adding a credential set

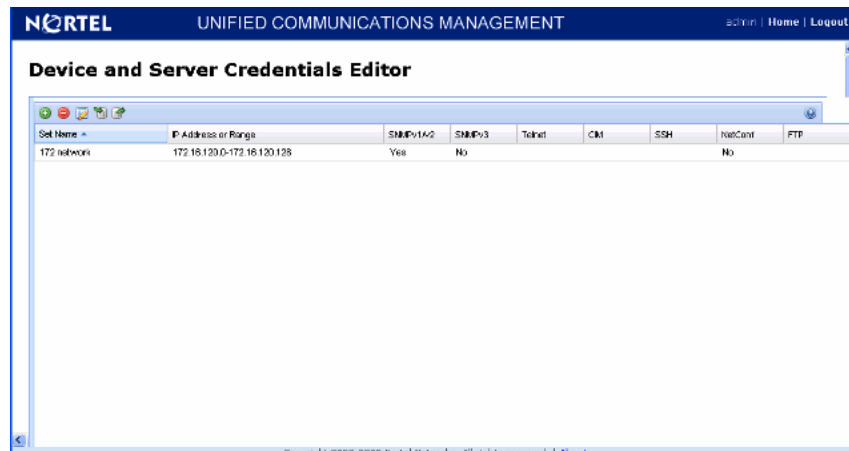
Perform the following procedure to add a new credential set to Unified Communications Management (UCM). You must add a credential set for each device you want to manage. The set name accepts printable ASCII characters, but not special characters (%(!)). You can enter the space ( ), dash (-), and underscore (\_) 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

Step	Action
------	--------

- 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 2 "Device and Server Credentials Editor fields"](#) (page 46).  
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.

---

—End—

---

### Adding a credential set for SNMPv3

Perform the following procedure to add credentials for SNMP v3.

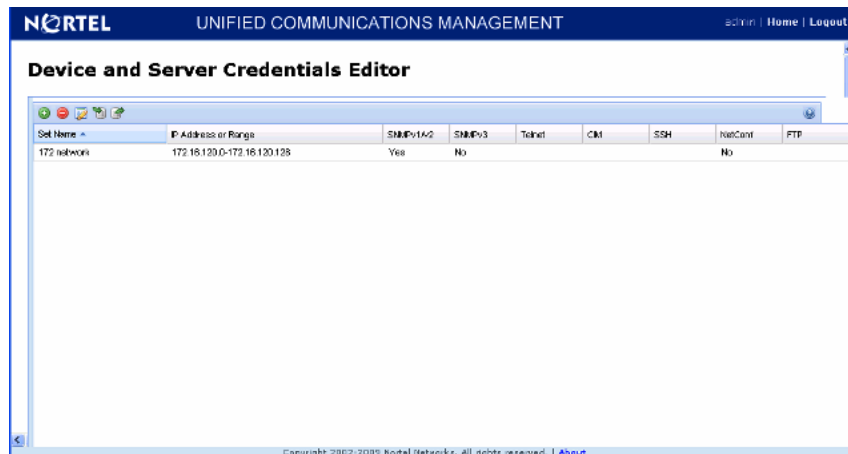
#### Procedure steps

Step	Action
------	--------

- |   |  |
|---|--|
| 1 | In the Navigation pane, expand <b>Admin</b> , and then click <b>Device Credentials</b> . |
|---|--|

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

—End—

## Deleting a credential set

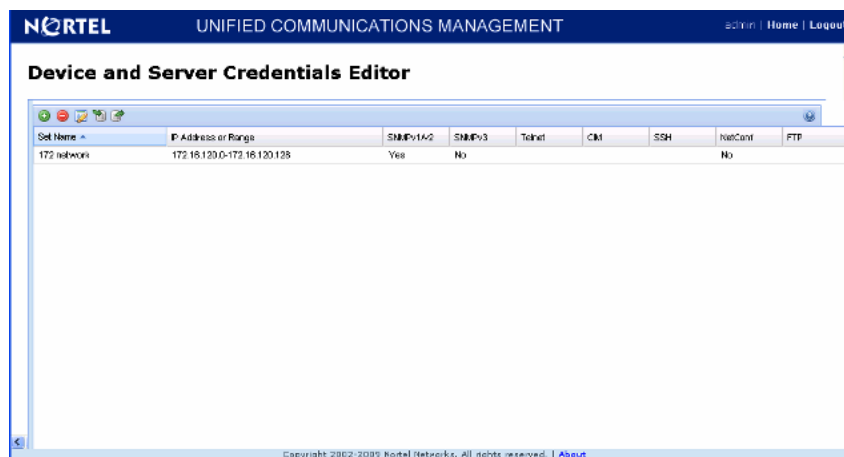
Perform the following procedure to remove a credential set from the Device and Server Credentials Editor.

### Procedure steps

Step	Action
------	--------

- 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**.

—End—

## Editing a credential set

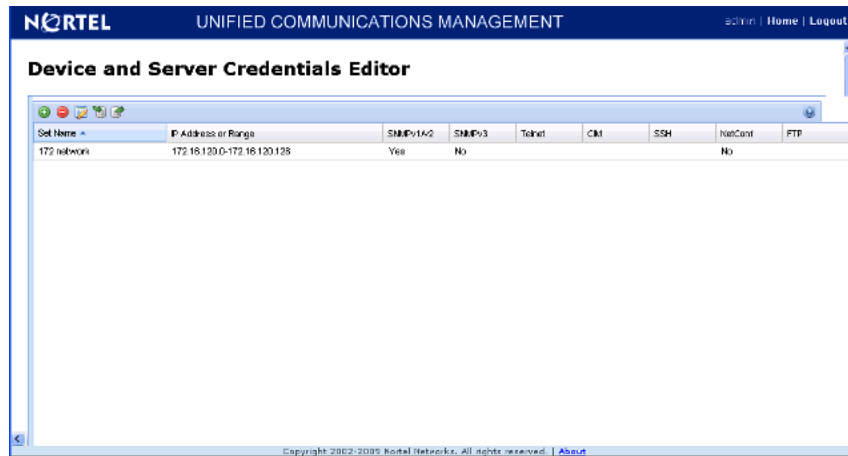
Perform the following procedure to edit a credential set to change the set name, IP address, and device credential information for a credential set.

### Procedure steps

Step	Action
------	--------

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

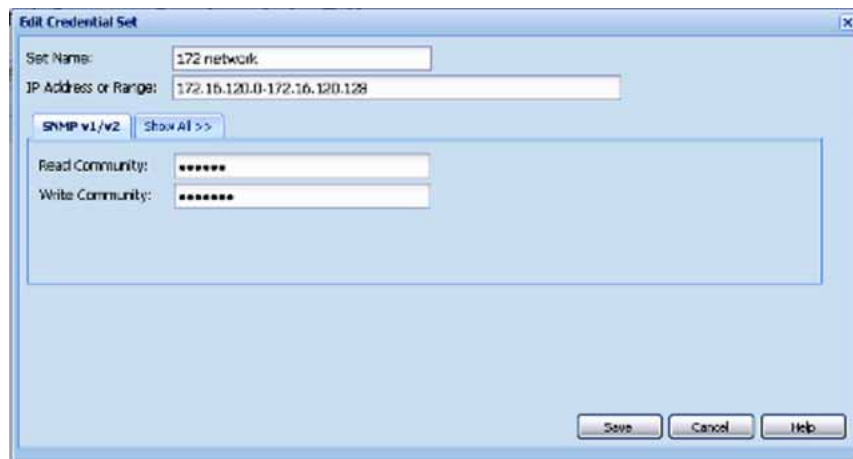
The Device and Server Credentials Editor page appears.



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.

—End—

## Importing a credential set

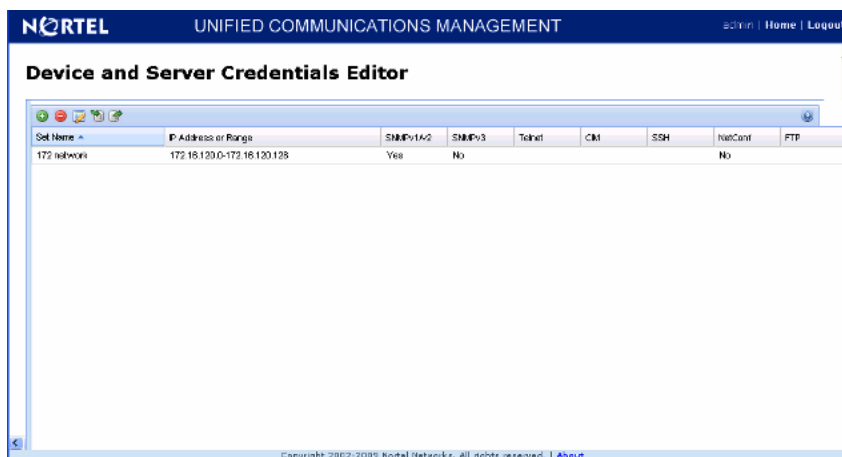
Perform the following procedure to import the credential set to the UCM.

### Procedure steps

Step	Action
------	--------

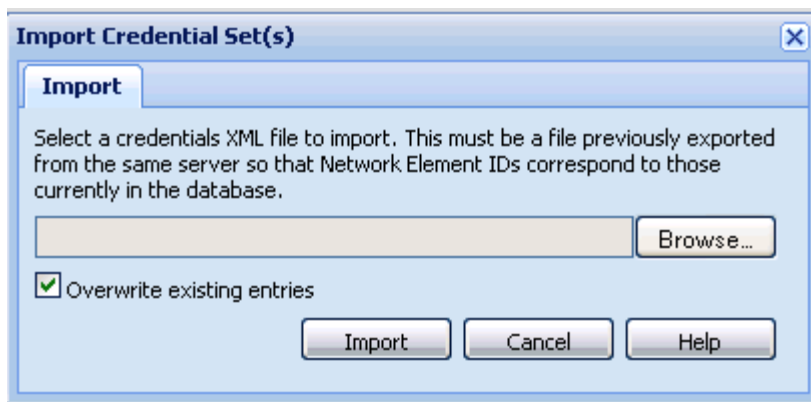
- 1 In the Navigation pane, expand **Admin**, and then click **Device Credentials**.

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**.

---

—End—

---

## Exporting a credential set

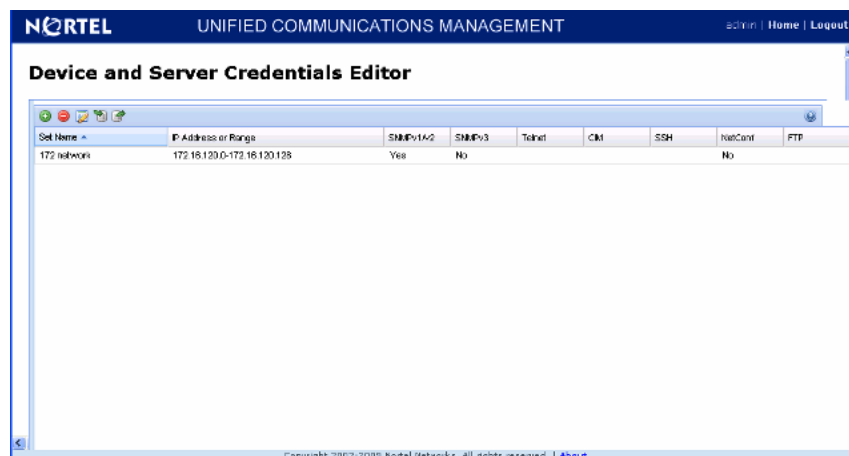
Perform the following procedure to export credential set from the UCM to a local XML file.

### Procedure steps

Step	Action
------	--------

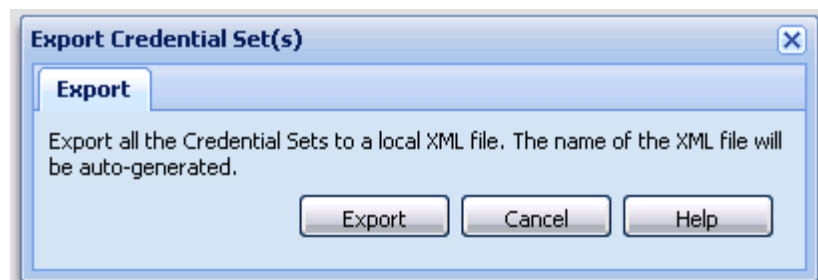
- 1 In the Navigation pane, expand **Admin**, and then click **Device Credentials**.

The Device and Server Credentials Editor page appears.



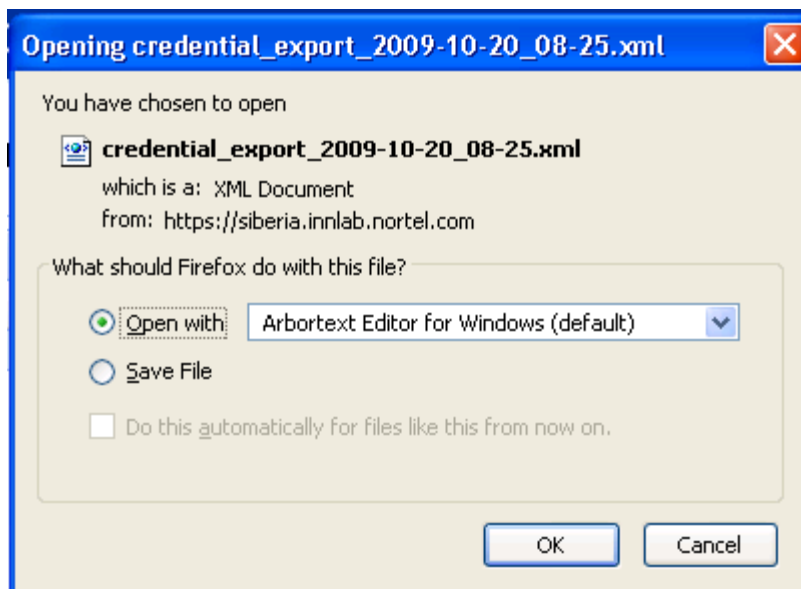
- 2 Click **Export Credentials**.

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**.

---

—End—

---

## 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

- ["Viewing existing users" \(page 54\)](#)
- ["Adding a new local or external user" \(page 55\)](#)
- ["Disabling an user" \(page 58\)](#)
- ["Deleting a user" \(page 58\)](#)

### Viewing existing users

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

## Procedure steps

Step	Action
------	--------

- 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.

**Administrative Users**

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

Add

<input type="checkbox"/>	User ID	Name	Roles	Type	Account Status
<input type="checkbox"/>	admin	Default security administrator	Administrator	Local	Enabled
<input type="checkbox"/>	sildefadmin	siladmin	UCMSystemAdministrator	Local	Enabled
<input type="checkbox"/>	sildefaur	sileraop	UCMOperator	Local	Enabled

- 2 View the information for existing users.

—End—

## 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

Step	Action
------	--------

- 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.

**Administrative Users**

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

<input type="checkbox"/>	User ID	Name	Roles	Type	Account Status
<input type="checkbox"/>	admin	Default security administrator	NetworkAdministrator	Local	Enabled
<input type="checkbox"/>	silbaadmin	silbaadmin	UCMSystemAdministrator	Local	Enabled
<input type="checkbox"/>	silbaop	silbaop	UCMOperator	Local	Enabled

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

**Add New Administrative User**

**Step 1:** Identify the new user.  
Enter the user's full name and select an authentication type and User ID. Locally authenticated users also require a temporary password.

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

Authentication Type:  Local  External

Full Name:

Temporary password:

Re-enter password:

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

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

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

- 3 In the **User ID** field, enter the user ID.
- 4 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.

### ATTENTION

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, Nortel 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.



**Add New Administrative User****Step2:** Assign Role(s)

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

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

Finish Cancel

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.

**ATTENTION**

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

—End—

**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

Step	Action
------	--------

- |   |   |
|---|---|
| 1 | In the Navigation pane, expand <b>Admin</b> , and then click <b>User Management</b> . |
|---|---|

The Administrative Users page appears.

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

**Administrative Users**

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

Buttons: Add, Remove, Refresh, Edit

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

- |   |  |
|---|--|
| 2 | In the <b>User ID</b> , select the User ID check box that you want to disable, and then click <b>Disable</b> . The Account Status for the selected user changes to Disabled. |
|---|--|

—End—

## Deleting a user

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

### Procedure steps

Step	Action
------	--------

- |   |   |
|---|---|
| 1 | In the Navigation pane, expand <b>Admin</b> , and then click <b>User Management</b> . |
|---|---|

The Administrative Users page appears.

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

**Administrative Users**

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

User ID	Name	Roles	Type	Account Status
<input type="checkbox"/> admin	Default security administrator	NetworkAdministrator	Local	Enabled
<input type="checkbox"/> silbaadmin	silbaadmin	UCMSystemAdministrator	Local	Enabled
<input type="checkbox"/> silbaaop	silbaaop	UCMOperator	Local	Enabled

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

### ATTENTION

Users cannot delete their own account.

—End—

## 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" (page 59)
- "Exporting a license" (page 60)
- "Generating a licensing report" (page 61)
- "Refreshing the license information" (page 62)

### Adding a license

Perform the following procedure to add a license.

#### Procedure steps

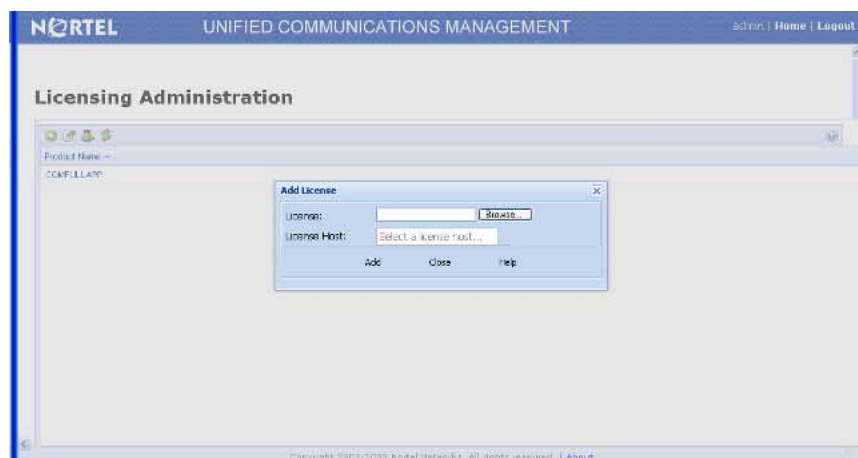
Step	Action
------	--------

- |   |  |
|---|--|
| 1 | In the Navigation pane, expand <b>Admin</b> panel, select <b>Licensing</b> .<br>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**.

---

—End—

---

### Exporting a license

Perform the following procedure to export a license file.

---

**Procedure steps**

---

**Step Action**

---

- 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.

---

—End—

---

**Generating a licensing report**

Perform the following procedure to generate a licensing report.

---

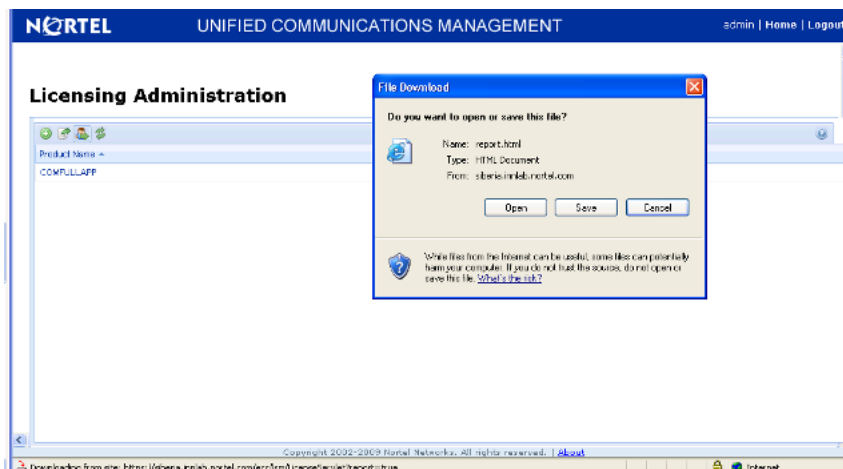
**Procedure steps**

---

**Step Action**

---

- 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.

---

—End—

---

### Refreshing the license information

Perform the following procedure to refresh the license information.

#### Procedure steps

Step	Action
------	--------

- |   |  |
|---|--|
| 1 | In the Navigation pane, expand <b>Admin</b> panel, and then click <b>Licensing</b> .<br>The Licensing Administration page appears. |
| 2 | In the product name table, select the product license to be exported.  |
| 3 | Click <b>Refresh</b> .   |

---

—End—

---

### 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 UCM 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" (page 63)
- "Installing EDM plugin" (page 63)
- "Uninstalling EDM plugin" (page 65)
- "Refreshing the plugin inventory table" (page 66)
- "Selecting the EDM preferences" (page 67)

## Downloading EDM plugin

Perform the following procedure to download an EDM plugin.

### Procedure steps

Step	Action
1	Open Nortel support site from the Web browser and select EDM Plugins section in <a href="http://support.nortel.com">http://support.nortel.com</a> .
2	Download <b>EDM Plugin</b> for a specific device type and version.
3	Click <b>Save</b> to save the plugin file on to disk, where you are running the web-browser.

—End—

## 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

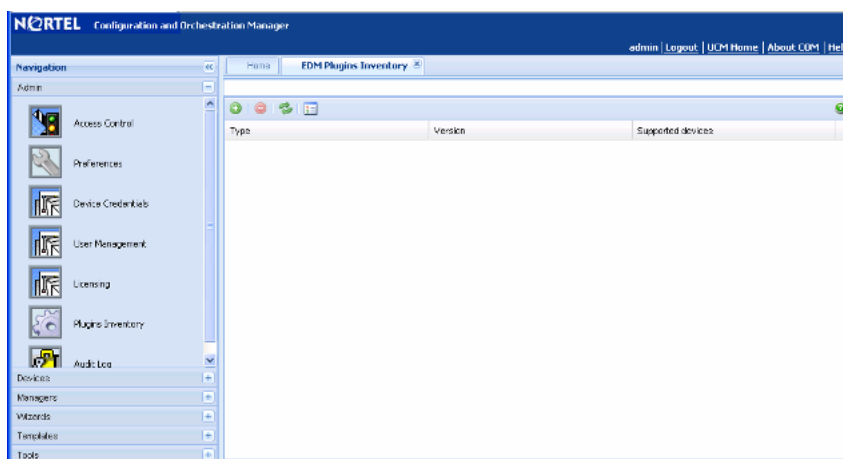
- You must have UCM administrator role or UCM system administrator role rights to access the Plugins Inventory.
- Ensure that you log on to COM as an administrator.

### Procedure Steps

Step	Action
------	--------

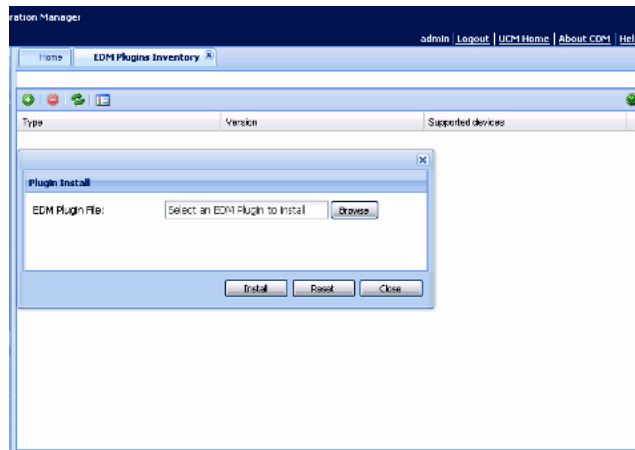
- |   |   |
|---|---|
| 1 | Download <b>EDM plugin</b> using the procedure, " <a href="#">Downloading EDM plugin</a> " (page 63). |
| 2 | From the Navigation pane, expand the <b>Admin</b> pane, and then click <b>Plugins Inventory</b> .     |

The EDM Plugins tab appears in the Contents pane.



- |   |   |
|---|---|
| 3 | Click <b>Install Plugin</b> .<br>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.

---

—End—

---

### 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 UCM 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

Step	Action
1	From the Navigation pane, expand the <b>Admin</b> pane, and then click <b>Plugins Inventory</b> .  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 <b>Uninstall Plugin</b> .  If the uninstallation is done successfully, the message "EDM Plugin uninstall" successful appears or an error message appears describing the problem.

---

—End—

---

### Refreshing the plugin inventory table

Perform the following procedure to refresh the plugin inventory table.

#### Prerequisites

- You must have UCM 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

Step	Action
1	Download <b>EDM plugin</b> using the procedure, " <a href="#">Downloading EDM plugin</a> " (page 63).
2	From the Navigation pane, expand the Admin pane, and then click <b>Plugins Inventory</b> .  The EDM Plugins tab appears in the Contents pane.
3	From the toolbar, click <b>Refresh Plugin Inventory</b> .  The Plugin Inventory table refreshes.

---

—End—

---

## Selecting the EDM preferences

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

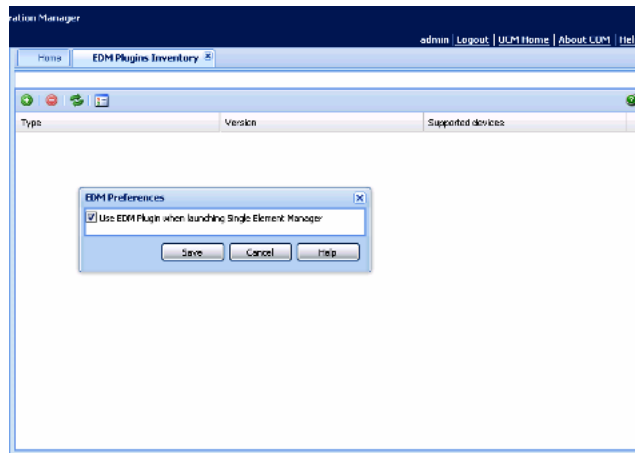
### Prerequisites

- You must have UCM 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

Step	Action
------	--------

- 1 Download **EDM plugin** using the procedure, "[Downloading EDM plugin](#)" (page 63).
- 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.

**ATTENTION**

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.

5 Click **Save**.

—End—

**Audit log**

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

**Navigation**

- "Launching the audit log" (page 68)
- "Refreshing audit logs" (page 69)

**Launching the audit log**

Perform the following procedure to start the audit log.

**Procedure steps****Step Action**

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

The Audit Log dialog box appears.

Date/Time	Debug Level	User	UserIP	Message
2009-08-04 00:17:40,690	INFO	admin		Listing installed plugins
2009-08-04 08:41:35,493	INFO	admin		Listing installed plugins
2009-08-04 08:39:40,990	INFO	admin		Listing installed plugins
2009-08-04 08:39:34,604	INFO	admin		Listing installed plugins
2009-08-04 08:38:48,196	INFO	admin		Listing installed plugins
2009-08-04 08:38:11,852	INFO	admin		Listing installed plugins
2009-08-04 06:04:20,877	INFO	admin		Listing installed plugins
2009-08-04 06:15:06,332	INFO	admin		Listing installed plugins
2009-08-04 06:09:02,252	INFO	admin		Listing installed plugins
2009-08-04 03:37:27,917	INFO	admin		Getting EDM preferences, value: true
2009-08-04 03:37:34,182	INFO	admin		Listing installed plugins

---

—End—

---

### Job aid

The following table shows the 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

Step	Action
------	--------

- |          |   |
|----------|---|
| <b>1</b> | From the Navigation pane, expand the Admin pane, and then click <b>Audit Log</b> .<br><br>The Audit Log dialog box appears. |
| <b>2</b> | Click <b>Refresh</b> .<br><br>The audit log details are refreshed.  |

---

—End—

---



## Devices management

The Device Inventory Manager lets you manage the 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**

Name	Reachable State	IP Address	Device Type	Version	Description	Time Stamp
ERS-8610	●	172.16.120.2	mERS8610	7.0.0.0	ERS-8610 (7.0.0.0)	2009-10-16 13:45:01
ERS-8606	●	172.16.120.5	mERS8606	7.0.0.0	ERS-8606 (7.0.0.0)	2009-10-16 13:45:01
SJ_PP1648T	●	172.16.120.8	mERS1648	2.1.5.0	ERS-1648T (2.1.5.0)	2009-10-16 13:45:01
5530-24TFD	●	172.16.120.17	mBPS2000	2.5.0.45	Business Policy Swi	2009-10-16 13:45:01
	●	172.16.120.24	mERS5530-24TFD	6.1.0.057	Ethernet Routing Sw	2009-10-16 13:45:01
4528	●	172.16.120.30	mERS2500-25T			2009-10-16 13:45:01
	●	172.16.120.38	mERS4526T	5.4.0.051	Ethernet Routing Sw	2009-10-16 13:45:01
	●	172.16.120.39	mERS4524GT			2009-10-16 13:45:01
	●	172.16.120.40	mERS4528FX			2009-10-16 13:45:01
ERS4548GTPWR	●	172.16.120.41	mERS4548GT-PWR	5.4.0.051	Ethernet Routing Sw	2009-10-16 13:45:01
ERS5000	●	172.16.120.62	mERS5650TD-PWR	6.1.0.057	Ethernet Routing Sw	2009-10-16 13:45:01
	●	172.16.120.100	mMLANSecuritySwi			2009-10-16 13:45:01
	●	192.167.1.1	mERS1648			2009-10-16 13:45:01
	●	192.167.1.17	mBPS2000	3.1.3.06	Business Policy Swi	2009-10-16 13:45:01

The following figure shows the Device Manager toolbar.

**Figure 16**  
**Device Manager toolbar**



The Device Inventory Manager allows you to

- add a device
- delete a device
- edit a device
- launch Element Manager
- import or export inventory
- refresh

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



---

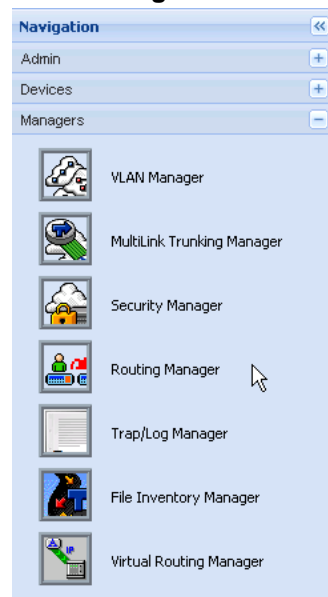
## Managers management

---

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

The following figures shows the Managers panel.

**Figure 17**  
**COM Managers**



The submanagers are described in the following sections:

- ["VLAN Manager" \(page 74\)](#)
- ["MultiLink Trunking Manager" \(page 74\)](#)

- "Security Manager" (page 75)
- "Routing Manager" (page 75)
- "Trap/Log Manager" (page 76)
- "File Inventory Manager" (page 76)
- "Virtual Routing Manager" (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 *Nortel 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 *Nortel 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 *Nortel 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 *Nortel 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 *Nortel 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 *Nortel 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 *Nortel Configuration and Orchestration Manager Administration — Utilities* (NN47226-600).



---

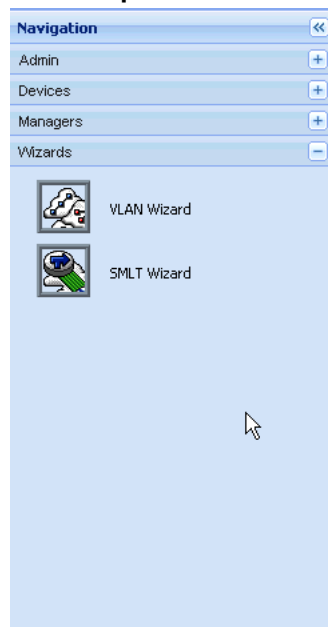
## Wizards management

---

The 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 two types of wizards:

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

The screenshot shows the 'VLAN Wizard' configuration window. The 'Steps' pane on the left highlights 'Add/Select STG'. The main area is titled 'Add/Select STG' and contains the following fields:

- STG Type:  Nortel STG,  RSTP,  MSTP
- Select:  New STG,  Existing STG
- ID:  [1 - 64]
- Type:  [Normal]
- Tagged BPDU Address:  [MAC address]
- Tagged BPDU Vlan ID:  [1 - 4094]
- Priority:  [0 - 65535]
- Bridge Max Age:  [600 - 4000 seconds]
- Bridge Hello Time:  [100 - 1000 seconds]
- Bridge Forward Delay:  [400 - 3000 seconds]
- Stp Enabled:
- Trap Enabled:
- Devices: Available Devices:  Selected Devices:

Buttons at the bottom include 'Load Template', 'Save as Template', 'Cancel', 'Previous', 'Next', 'Finish', and 'Help'.

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

The screenshot shows the 'SMLT Wizard' configuration window. The 'Steps' pane on the left highlights 'Select Switches'. The main area is titled 'Select Switches' and contains the following fields:

- Switch Type:
- Switch 1:
- Switch 2:

Buttons at the bottom include 'Load Template', 'Save as Template', 'Cancel', 'Previous', 'Next', 'Finish', and 'Help'.

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

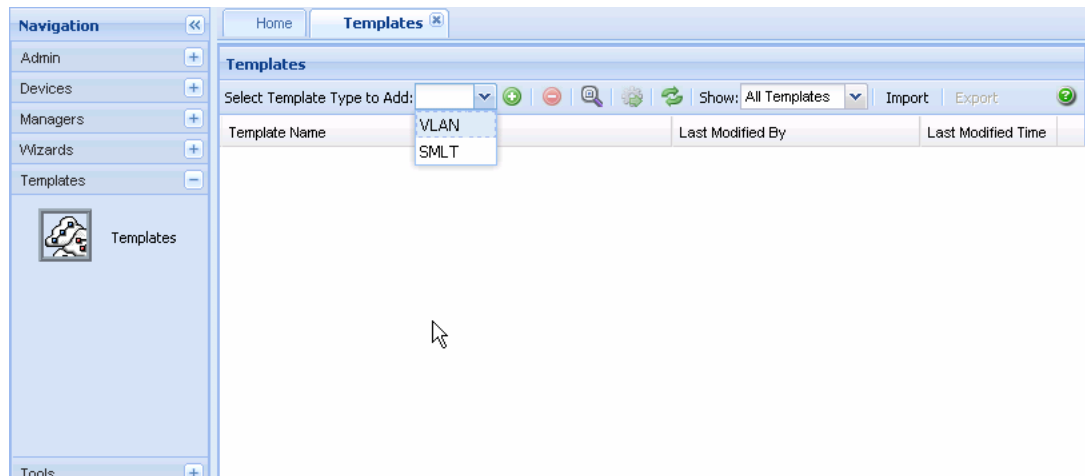


## Templates management

The template contains a set of configuration attributes. Templates can be created by running the 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.



There are two 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

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

---

# Tools management

---

This chapter provides information about SmartDiff Tool, TFTP Server, MIB Browser, Port Scanner, and Scheduled Tasks tools supported by Configuration and Orchestration Manager (COM).

## Navigation

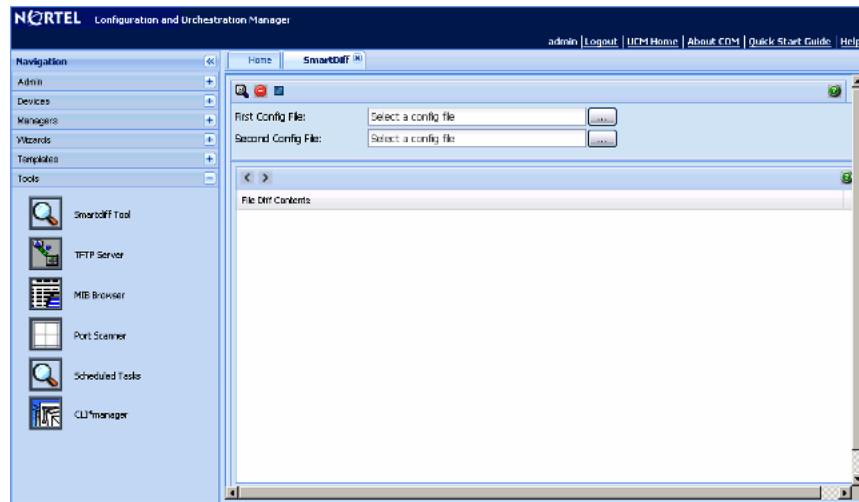
- "SmartDiff Tool" (page 83)
- "TFTP Server" (page 85)
- "MIB Browser" (page 90)
- "Port Scanner" (page 98)
- "Scheduled Tasks" (page 100)
- "CLI\*manager" (page 102)

## 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

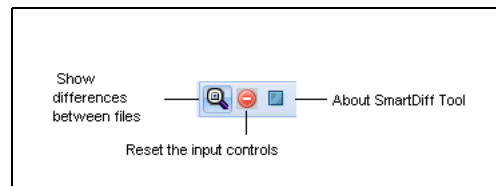
Step	Action
1	In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>SmartDiff Tool</b> icon.  The SmartDiff dialog box appears.



—End—

The following figure shows the SmartDiff toolbar.

**Figure 19**  
SmartDiff toolbar



## Comparing configuration files

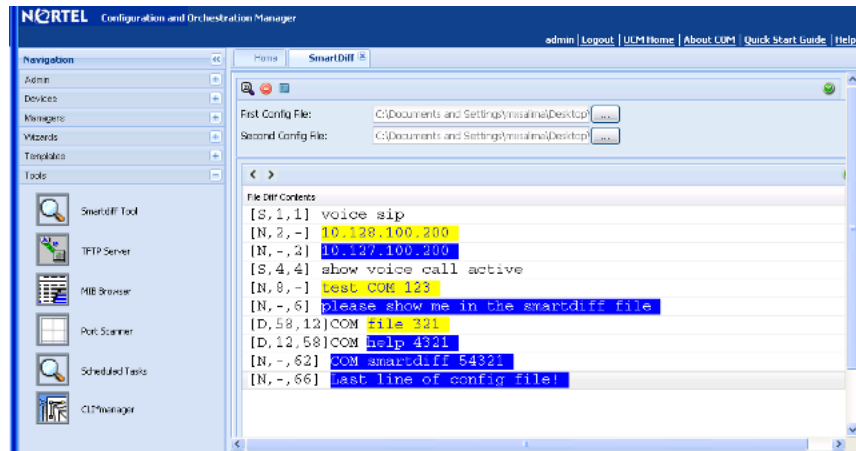
Perform the following procedure to compare two configuration files.

### Procedure steps

Step	Action
------	--------

- |   |  |
|---|--|
| 1 | In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>SmartDiff Tool</b> icon.  |
| 2 | In <b>First Config File</b> and <b>Second Config File</b> fields, enter the name of the configuration files you want to compare. Use the ... buttons to browse the files.<br><br>Click <b>Reset the input controls</b> to reset the <b>First Config File</b> and <b>Second Config File</b> fields value. |
| 3 | Click the <b>Show differences between files</b> 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.

---

—End—

---

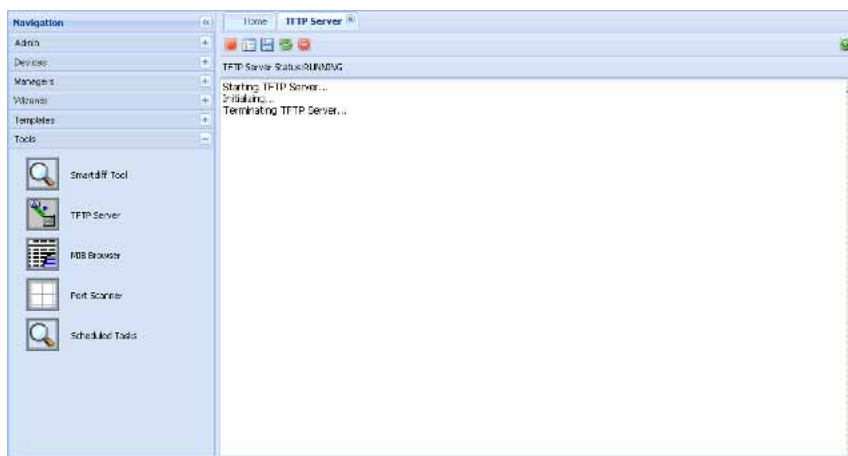
## TFTP Server

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

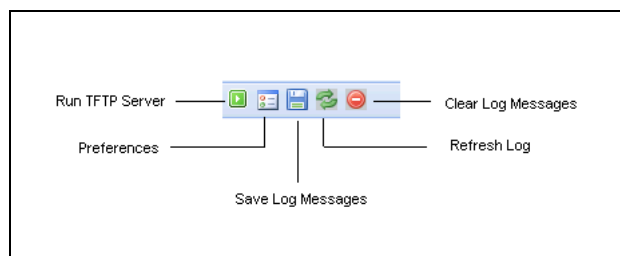
- | Step | Action   |
|------|--|
| 1    | In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>TFTP Server</b> icon.<br>The TFTP Server tab appears. |



—End—

The following figure shows the TFTP Server toolbar.

**Figure 20**  
**TFTP Server toolbar**



## Navigation

- "Viewing the status of TFTP Server" (page 87)
- "Starting and stopping TFTP Server" (page 87)
- "Editing preferences" (page 88)
- "Saving log messages" (page 89)
- "Refreshing log messages" (page 89)

- "Clearing log messages" (page 90)

## Viewing the status of TFTP Server

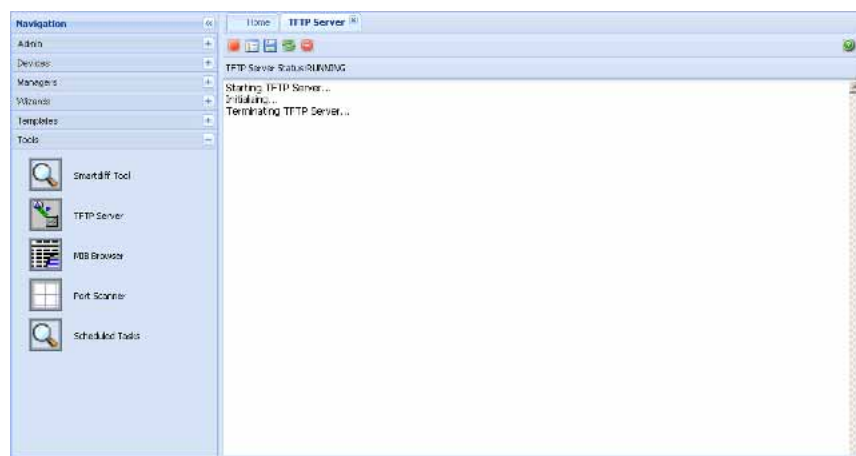
Perform the following procedure to view the status of the TFTP server.

### Procedure steps

Step	Action
------	--------

- |   |  |
|---|--|
| 1 | In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>TFTP Server</b> icon. |
|---|--|

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



—End—

## Starting and stopping TFTP Server

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

### Procedure steps

Step	Action
------	--------

- |   |  |
|---|--|
| 1 | In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>TFTP Server</b> icon.<br><br>The TFTP Server tab appears.   |
| 2 | If the TFTP Server Status is running, click <b>Stop TFTP Server</b> from the toolbar to stop the TFTP Server. After stopping the TFTP Server, this button turns to <b>Start TFTP Server</b> .<br><b>OR</b> |

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** .

---

—End—

---

## Editing preferences

Perform the following procedure to edit TFTP Server preferences.

### Procedure steps

Step	Action
------	--------

- |   |  |
|---|--|
| 1 | In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>TFTP Server</b> icon.<br><br>The TFTP Server tab appears. |
| 2 | Click <b>Preferences</b> from the toolbar.<br>The TFTP Server Preferences dialog box appears, as shown in the following figure.        |

- |   |  |
|---|--|
| 3 | Update the field you want to modify, and then click <b>OK</b> to commit the changes or click <b>Cancel</b> to discard the changes. |
|---|--|

---

—End—

---

## Job aid

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



**Table 3**  
**TFTP Server Preferences table**

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

### Saving log messages

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

#### Procedure steps

Step	Action
1	In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>TFTP Server</b> icon.  The TFTP Server tab appears.
2	Click <b>Save Log Messages</b> from the toolbar to save the current TFTP server log.

—End—

### Refreshing log messages

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

#### Procedure steps

Step	Action
1	In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>TFTP Server</b> icon.  The TFTP Server tab appears.
2	Click <b>Refresh Log</b> from the toolbar to refresh the current TFTP server log.

—End—

## Clearing log messages

Perform the following procedure to clear the TFTP server log.

### Procedure steps

Step	Action
------	--------

- |   |  |
|---|--|
| 1 | In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>TFTP Server</b> icon.<br><br>The TFTP Server tab appears.                                   |
| 2 | Click <b>Clear Log Messages</b> from the toolbar. After you are prompted to confirm the clearing of log messages, click <b>Yes</b> to clear the current TFTP server log. |

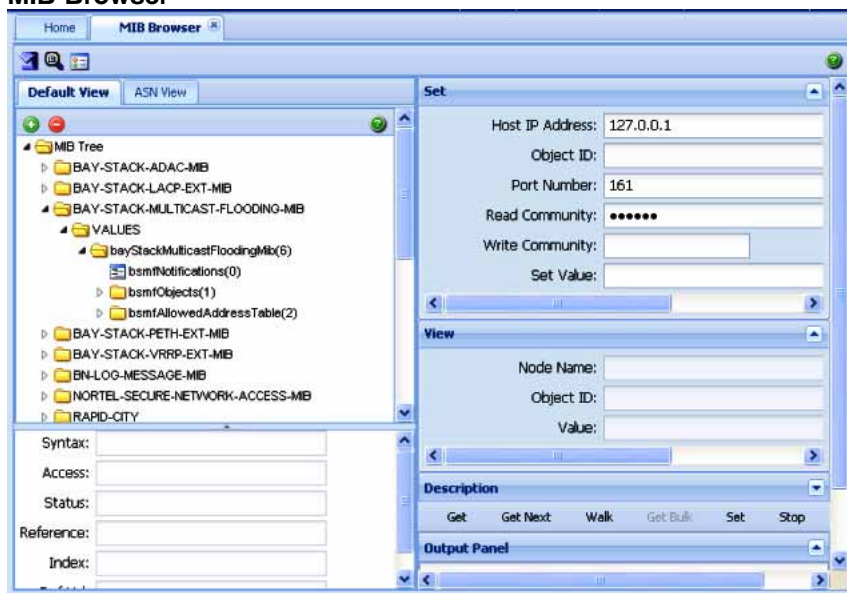
—End—

## 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 21**  
**MIB Browser**









The following table describes the parts of MIB Browser tab.

**Table 4**  
**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 5**  
**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: <ul style="list-style-type: none"> <li>• SNMP v1</li> <li>• SNMP v2c</li> <li>• SNMP v3</li> </ul>
SNMP Bulk Settings		Opens Get Bulk Panel.
SNMPV3 Settings		Opens SNMPV3 Panel.
Help		Opens Online Help.

## Navigation

- ["Loading an MIB" \(page 92\)](#)
- ["Unloading an MIB" \(page 92\)](#)
- ["Setting SNMP version" \(page 93\)](#)

- "Retrieving data of an MIB node" (page 94)
- "Traversing MIB tree" (page 95)
- "Retrieving value of a subtree" (page 95)
- "Retrieving data from a large table" (page 96)
- "Editing data for MIB node" (page 96)

## Loading an MIB

Perform the following procedure to load an MIB.

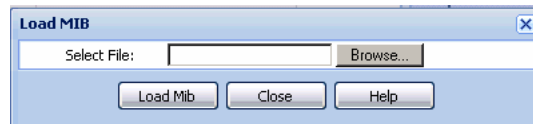
### Procedure steps

---

Step	Action
------	--------

---

- 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.

---

—End—

---

## Unloading an MIB

Perform the following procedure to unload an MIB.

---

### Procedure steps

Step	Action
1	In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>MIB Browser</b> icon.  The MIB Browser tab appears.
2	Click the <b>Default view</b> tab and select the MIB node you want to delete.
3	Click the <b>Unload MIB</b> icon from the toolbar. After you are prompted to confirm the unloading.
4	Click <b>Yes</b> to unload the selected MIB. <b>OR</b> Click <b>No</b> to cancel the unload operation.  The MIBs will be removed from the tree if you click Yes.

---

—End—

---

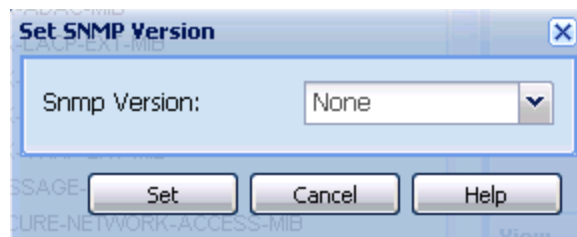
### Setting SNMP version

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

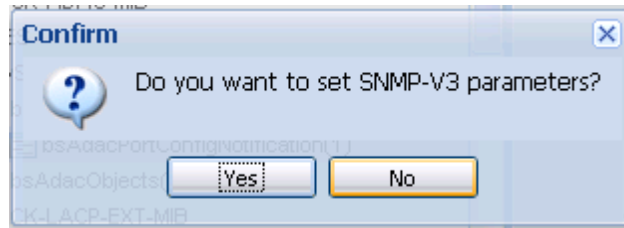
---

### Procedure steps

Step	Action
1	In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>MIB Browser</b> icon.  The MIB Browser tab appears.
2	Click the <b>Default view</b> or <b>ASN View</b> tab and select an MIB which SNMP you wish to change.
3	Click the <b>Set SNMP Version</b> icon from the toolbar. The Set SNMP Version dialog box appears.



- 4 Choose the version that you wish to set in the **Snm 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.

---

—End—

---

### Retrieving data of an MIB node

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

---

### Procedure steps

---

Step	Action
------	--------

---

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

—End—

---

### Traversing MIB tree

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

---

### Procedure steps

---

Step	Action
------	--------

---

- |   |   |
|---|---|
| 1 | In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>MIB Browser</b> icon. The MIB Browser tab appears. |
| 2 | Select the desired node from the MIB tree.  |
| 3 | Click <b>Get Next</b> from the menubar.   |
- 

—End—

---

### Retrieving value of a subtree

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

---

### Procedure steps

---

Step	Action
------	--------

---

- |   |   |
|---|---|
| 1 | In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>MIB Browser</b> icon. The MIB Browser tab appears. |
| 2 | Select the desired node from the MIB tree.  |
| 3 | Click <b>Walk</b> from the menubar.   |
- 

—End—

---

## Retrieving data from a large table

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

### ATTENTION

The GetBulk operation is applicable only on SNMPv2c and SNMPv3.

### Procedure steps

Step	Action
1	In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>MIB Browser</b> 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 " <a href="#">Setting SNMP version</a> " (page 93).
4	Click <b>SNMP Bulk Setting</b> 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 <b>Add</b> .
6	Enter the value in <b>Max. Repetitions</b> and <b>Non Repeaters</b> fields.
7	Click <b>Get Bulk</b> 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.



—End—

## Editing data for MIB node

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

### ATTENTION

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



### Procedure steps

Step	Action
1	In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>MIB Browser</b> 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 <b>Set Value</b> field of <b>Set</b> panel.
4	Click <b>Set</b> from the menubar.

—End—

### Job aid

The following table describes the fields of 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.

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

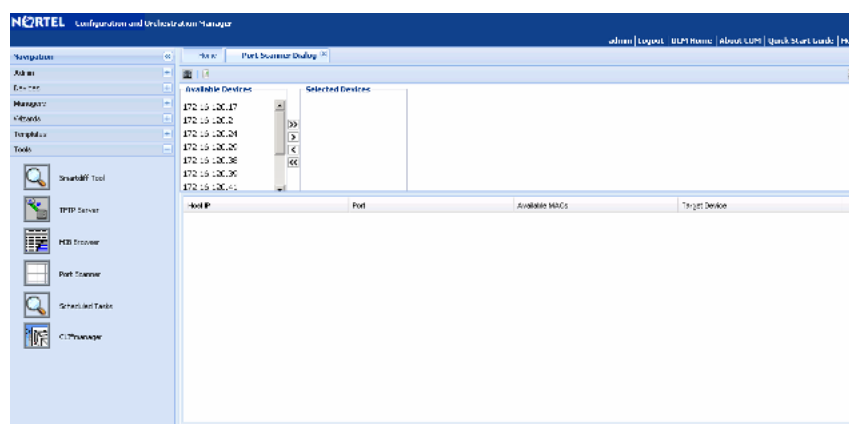
Port Scanner allows you to scan the target devices. Port Scanner enables parameters to configure periodic port scan, and store exported port scan data into files. Perform the following procedure to view the Port scanner dialog box.

### Procedure steps

Step	Action
------	--------

- |   |   |
|---|---|
| 1 | In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>Port Scanner</b> icon. |
|---|---|

The Port Scanner dialog box appears.



—End—

### Navigation

- "Scanning Ports" (page 98)
- "Exporting report of port scan" (page 99)

### Scanning Ports

Perform this procedure to scan ports of the selected device.

### Procedure steps

Step	Action
------	--------

- |   |  |
|---|--|
| 1 | In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>Port Scanner</b> 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.

---

—End—

---

### Exporting report of port scan

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

#### Procedure steps

Step	Action
1	In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>Port Scanner</b> icon. The Port Scanner dialog box appears.
2	Select the devices, you wish to scan, in the <b>Available Device</b> field, and move to <b>Selected Devices</b> using > or >>.
3	Click the <b>Scan Ports</b> icon from the tool bar. The result is displayed in the content pane.
4	Click <b>Export</b> icon from the tool bar to export the report. The Export dialog box appears.
5	Select the type (html, or text) in <b>Export type</b> field, and then click <b>Ok</b> .

---

—End—

---

### Job aid

The following table describes the parts of Port Scanner tab.

Part	Description
Toolbar	Provides you Scan Port and Export tools. <ul style="list-style-type: none"> <li>• Scan Port—allows you to scan the target devices.</li> <li>• Export—allows you to export the result in text format.</li> </ul>
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.

Part	Description
>	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

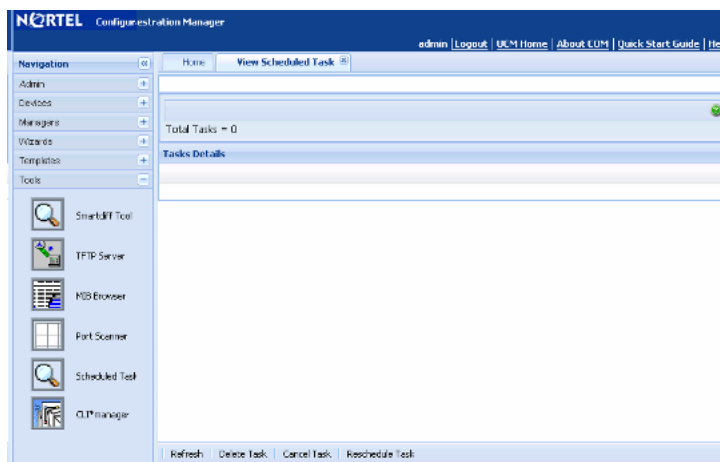
Using Sceduled Tasks tool, you can only view, delete, cancel or re-schedule tasks from the File Inventory Manager. Perform the following procedure to view the scheduled tasks.

### Procedure steps

Step	Action
------	--------

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

The Scheduled Tasks dialog box appears.



—End—

The following table describes the tools of Scheduled Tasks tab.

**Table 6**  
**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" \(page 101\)](#)
- ["Deleting a scheduled task" \(page 101\)](#)
- ["Canceling a scheduled task" \(page 102\)](#)
- ["Rescheduling a scheduled task" \(page 102\)](#)

## Refreshing scheduled task list

Perform the following procedure to refresh the scheduled task list.

### Procedure steps

Step	Action
1	In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>Scheduled Tasks</b> icon. The View Scheduled Task tab appears listing all the scheduled tasks.
2	Click <b>Refresh</b> to refresh the list.
—End—	

## Deleting a scheduled task

Perform the following procedure to delete a scheduled task.

### Procedure steps

Step	Action
1	In the Navigation pane, select the <b>Tools</b> panel, and then click the <b>Scheduled Tasks</b> 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.

---

—End—

---

### Canceling a scheduled task

Perform the following procedure to cancel a scheduled task.

#### Procedure steps

---

Step	Action
------	--------

---

- 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.

---

—End—

---

### Rescheduling a scheduled task

Perform the following procedure to reschedule a scheduled task.

#### Procedure steps

---

Step	Action
------	--------

---

- 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.

---

—End—

---

## CLI\*manager

CLI\*manager speeds up and simplifies operations and provisioning for a large number of Nortel 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

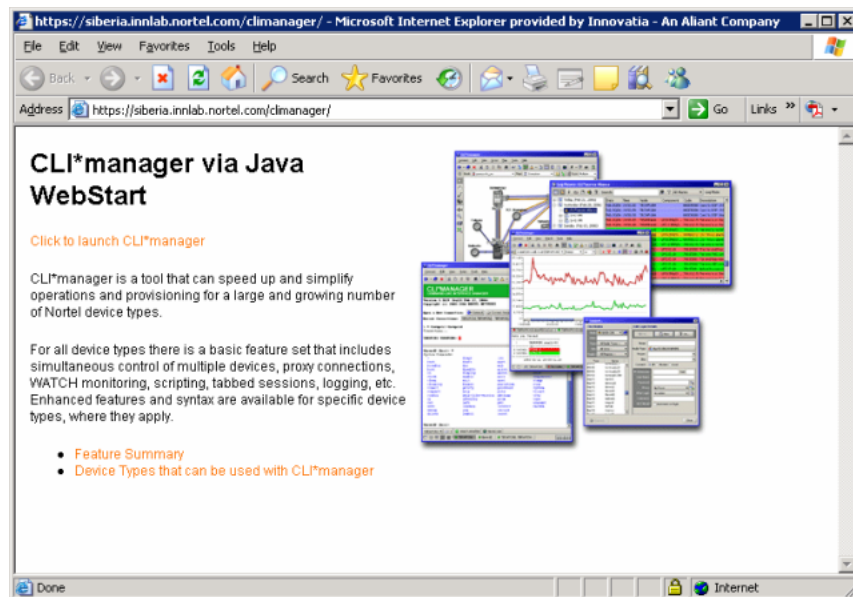
- You must install Java Virtual Machine (JVM).

Perform the following procedure to launch the CLI\*manager.

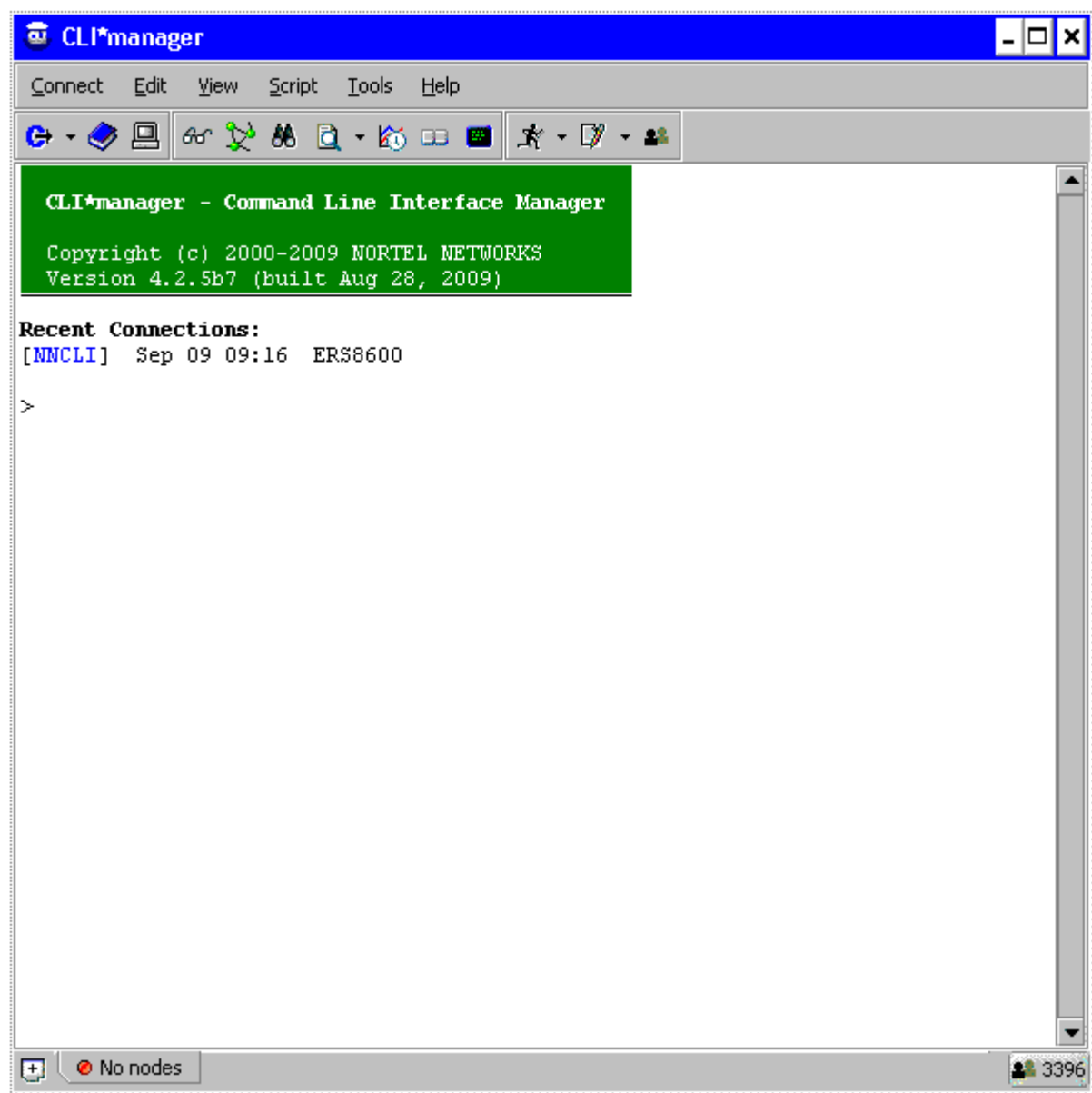
## Procedure steps

Step	Action
------	--------

- 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.



---

—End—

---

## Navigation

- "CLI\*manager user interface" (page 105)
- "Connection set up" (page 105)
- "Supported device type" (page 106)



## 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
  - Metro Ethernet Switching Unit 1800/1860
  - Nortel Secure Router 1000, 3120, 6230,6280
  
- 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-Nortel
  - 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
  - WLAN Access Point 2220/2221/2300
  - WLAN Security Switch 2700

---

## Appendix

# Recommendations and deployments

---

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

- "COM installation server" (page 109)
- "Rediscoveries and device assignments" (page 109)
- "Internet browser Settings" (page 110)
- "License upgrades and device inventory" (page 111)

### 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

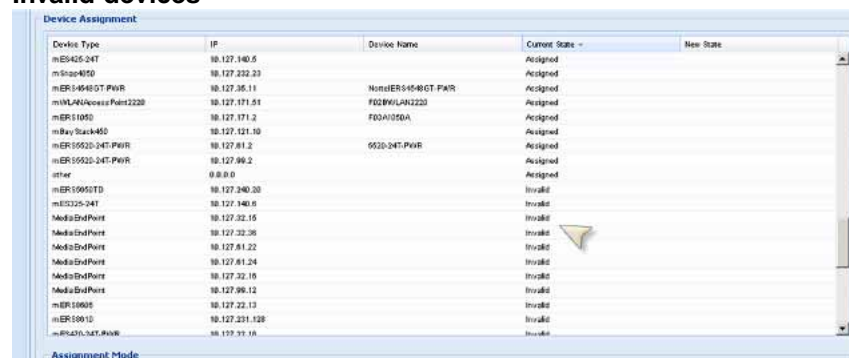
Network rediscoveries may result in 2 scenarios.

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 22**  
Invalid devices

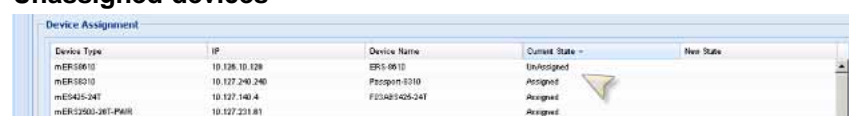


Device Type	IP	Device Name	Current State	New State
mES425-24T	10.127.140.5		Assigned	
mSnap4050	10.127.232.23		Assigned	
mER10540T-PWR	10.127.35.11	NorthER10540T-PWR	Assigned	
mER10540Access-Port2220	10.127.171.51	FD0HWLAN2220	Assigned	
mER11050	10.127.171.2	FD0HW1050A	Assigned	
mBay-Stack-450	10.127.121.10		Assigned	
mER10520-24T-PWR	10.127.81.2	0520-24T-PWR	Assigned	
mER10520-24T-PWR	10.127.96.2		Assigned	
other	0.0.0.0		Assigned	
mER1050TD	10.127.240.30		Invalid	
mES225-24T	10.127.140.6		Invalid	
Media-EndPoint	10.127.32.15		Invalid	
Media-EndPoint	10.127.32.38		Invalid	
Media-EndPoint	10.127.81.22		Invalid	
Media-EndPoint	10.127.81.24		Invalid	
Media-EndPoint	10.127.32.10		Invalid	
Media-EndPoint	10.127.96.12		Invalid	
mER10605	10.127.22.13		Invalid	
mER10910	10.127.231.128		Invalid	
mER420-3MT-PWR	10.157.31.16		Invalid	

- 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 23**  
Unassigned devices



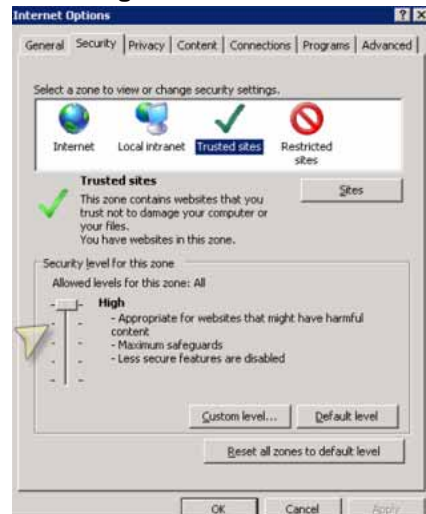
Device Type	IP	Device Name	Current State	New State
mER10610	10.128.10.128	ERS-0610	Unassigned	
mER10810	10.127.240.240	Procpwr-0210	Assigned	
mES425-24T	10.127.140.4	FD0481425-24T	Assigned	
mER10500-24T-PWR	10.127.231.81		Assigned	

## 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 24**  
**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.

## License upgrades and device inventory

COM base license must be upgraded to a COMFULLAPP (Full application license) for deployments. COM full application license has network discovery capabilities. When you reinstall a license, the devices that were manually added are dropped.

Deployments that are using COMFULLAPP license, but choose to downgrade only to COM license will lose all devices and will have to start adding the devices to management manually via manual device insertion in Device Inventory screens. In downgrade scenario, you are required to uninstall and then re-install COM.

---

# Index

---

## F

File-Inventory Manager  
features 76

## L

Latest logs pane 24  
Links 25  
Logging in 27

## M

Max Hops field 44  
MIB Browser 90  
MLT Manager, features 74

## N

network topology map  
viewing separate networks 44

## P

Port Scanner 98

## R

Restrict Discovery field 44

Routing Manager 75

## S

Scheduled Tasks 100  
Security Manager  
features 75  
Seed Address(es) item 44  
SmartDiff 83  
SNMP Listen for Traps item 44  
SNMP Max Outstanding Requests item 44  
SNMP Retry Count item 44  
SNMP Timeout item 44

## T

TFTP Server  
setting default for 45  
Tftp server 85  
Trap/Log Manager 76

## V

VLAN Manager features 74  
VRF Manager 77





Nortel Configuration and Orchestration Manager

## Using the Product Interfaces

Copyright © 2009, Nortel Networks  
All Rights Reserved.

Publication: NN47226-100  
Document status: Standard  
Document version: 01.01  
Document date: 2 November 2009

To provide feedback or report a problem in this document, go to [www.nortel.com/documentfeedback](http://www.nortel.com/documentfeedback)

Sourced in Canada and the United States of America

The information in this document is subject to change without notice. Nortel Networks reserves the right to make change in design or components as progress in engineering and manufacturing warrant.

\*Nortel, Nortel Networks, the Nortel logo and the Globemark are trademarks of Nortel Networks.

