Cisco Monitor Manager Application Configuration Guide, Release 1.5

First Published: February 24, 2014

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-31561-01

CONTENTS

Preface

This preface contains the following sections:

Audience

This guide is intended for site administrators who will manage Cisco Smart-enabled software installation and licensing.

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.

Convention	Description
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

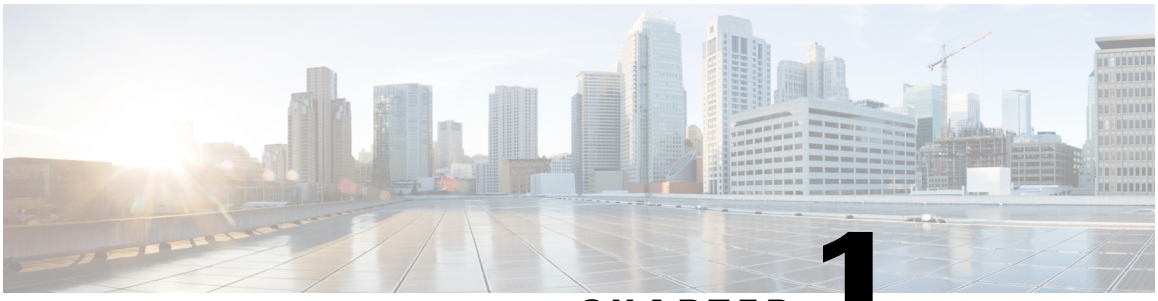
Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.



CHAPTER 1

Cisco Monitor Manager Overview

This chapter contains the following sections:

About Cisco Extensible Network Controller

Cisco Extensible Network Controller (Cisco XNC) is a software platform that serves as an interface between the network elements (southbound) and third-party applications (northbound). Cisco XNC is a JVM-based application that runs on a Java Virtual Machine (JVM). Cisco XNC is based on a highly available, scalable, and extensible architecture that supports a network. Cisco XNC is built for extensibility using the Open Services Gateway initiative (OSGi) framework, which allows new functionality to be added.

Cisco XNC can support multiple protocol plugins in the southbound direction. In the current release, Cisco Plug-in for OpenFlow 1.0 is available.

Cisco XNC provides the following:

- Multiprotocol capability with the Cisco Plug-in for OpenFlow version 1.0 available in this release.
- Functionality to support network visibility and programmability, such as network topology discovery, network device management, forwarding rules programming, and access to detailed network statistics.
- A Service Abstraction Layer (SAL) that enables modular southbound interface support, such as OpenFlow.
- Consistent management access through the GUI or through Java or Representational State Transfer (REST) northbound APIs.
- Security features, such as role-based access control (RBAC), and integration with an external Active Directory using RADIUS or TACACS for authentication, authorization, and accounting (AAA) functions.
- Troubleshooting tools, such as analytics gathering and diagnostic packet injection.

- Cisco advanced features such as Topology Independent Forwarding (TIF), which enables the administrator to customize the path a data flow takes through the network.
- Cisco network applications such as Network Slicing that allows logical partitioning of the network using flow specification, and Monitor Manager, that provides visibility into the network traffic.
- High-availability clustering to provide scalability and high availability.
- The Cisco Open Network Environment Platform Kit (Cisco onePK) version 1.1.0 is supported in this release of Cisco XNC. The Cisco onePK plug-in communicates with the onePK agent.
- Support for onePK devices in the network and the ability to install TIF rules on onePK devices.
- A CLI framework for Cisco XNC.
- Virtual Patch Panel Application (P2P Forwarding application) provides port-to-port traffic management within a switch or across the network without any need for physical connection changes or rewiring.

About Cisco Monitor Manager

Cisco Monitor Manager is a network application that runs on Cisco XNC. Cisco Monitor Manager, in combination with the Cisco Plug-in for OpenFlow and Cisco Nexus 3000 or 3100 Series switches and , enables you to create a scalable and flexible replacement for matrix switches, which traditionally connect network monitoring devices to points within the network where monitoring is desired.

Cisco Monitor Manager provides management support for multiple disjointed Cisco Monitor Manager networks. You can manage multiple Monitor Manager topologies that may be disjointed using the same Cisco XNC instance. For example, if you have 5 data centers and want to deploy an independent Cisco Monitor Manager solution for each data center, you can manage all these 5 independent deployments using a single Cisco XNC instance by creating a logical partition (network slice) for each monitoring network.

With the Cisco Monitor Manager solution, you can do the following:

- Classify Switched Port Analyzer (SPAN) and Test Access Point (TAP) ports.
- Filter which traffic should be monitored.
- Redirect packets from a single or multiple SPAN or TAP ports to multiple monitoring devices through delivery ports.
- Restrict which users can view and modify the monitoring system.

Configuring User Roles for Edge Ports

To manage which Cisco Monitor Manager application users may create rules for edge ports, you must modify the App-User role settings in the config.ini file. This allows you to enable Role-Based Access Control (RBAC) for application users. After you make the change and Cisco XNC is restarted, the following restrictions will be in force:

- Cisco Monitor Manager App-User role users will be able to create rules only for source ports associated to their role and only for ports assigned to their groups.
- Only Cisco Monitor Manager App-Admin role users will be able create rules with no source.

To enable RBAC for the App-User role, follow these steps:

Step 1 Open the config.ini file for editing.

Step 2 Locate the line `#Enforce restriction on edge/tap ports user can capture (default failse).`

Step 3 Remove the comment character from the following line:
`monitor.strictAuthorization=true`

Step 4 Save your work and close the file.

Step 5 If Cisco XNC is running, restart the application to enable the change.

Logging in to the Cisco Monitor Manager GUI

You can log into the Cisco Monitor Manager using HTTP or HTTPS:

- The default HTTP web link for the Cisco Monitor Manager GUI is `http://Controller_IP:8080/monitor`
- The default HTTPS web link for the Cisco Monitor Manager GUI is `https://Controller_IP:8443/monitor`

Note Before you can use HTTPS, you must manually specify the https:// protocol in your web browser. The controller must also be configured for HTTPS.

Step 1 In your web browser, enter the Cisco Monitor Manager web link.

Step 2 On the launch page, do the following:

a) Enter your username and password.
The default username and password is admin/admin.

b) Click **Log In**.

Cisco Monitor Manager GUI Overview

The Cisco Monitor Manager GUI contains the following areas and panes:

- A menu bar across the top of the window that provides access to the main categories of information in Cisco Monitor Manager.
- A topology map on the right that displays a visual representation of your network.

- Several panes with additional views and information about the selected category.

The menu bar contains the following items:

- The administrative management list—Provides access to different administrative settings, including managing roles and resource groups.

Note This drop-down list displays the username that you used when you logged into Cisco Monitor Manager. In this documentation, it will be referred to as the **Admin** drop-down list.

- A **Save** button to save any additions or changes made in the Monitor Manager application.

Topology Tools

The left side of the topology pane contains a group of tools that allow you to manipulate the content of the topology pane. Hovering over a tool displays its function. From the top of the pane to the bottom, the tools are:

- Move mode—Use this tool to move the entire topology diagram, a single topology element, or a node group. To move an element or a node group, click it and drag it.
- Zoom in—Use this tool to increase the size of the topology diagram.

Note You can also increase the size of the topology diagram by scrolling up with your mouse wheel.

- Zoom out—Use this tool to decrease the size of the topology diagram.

Note You can also decrease the size of the topology diagram by scrolling down with your mouse wheel.

- Zoom by selection—Use this tool to zoom in on a specific topology element. To zoom by selection, click the tool, then click and drag your mouse across the element you want to zoom in on. The zoom element display resets after a few seconds.
- Fit stage—Use this tool to reset the topology diagram in the topology pane.
- Topology Settings—Use this tool to choose the preferred **Display Icons as dots** setting. Select the radio button for the preference you desire.
- Tool tips–Tool tips display information about each tool, or about nodes in the topology. To display tool tip information, hover over a tool or over a node in the diagram.

Pane Resizing

You can resize the panes in the GUI display by clicking the pane resize grippers.

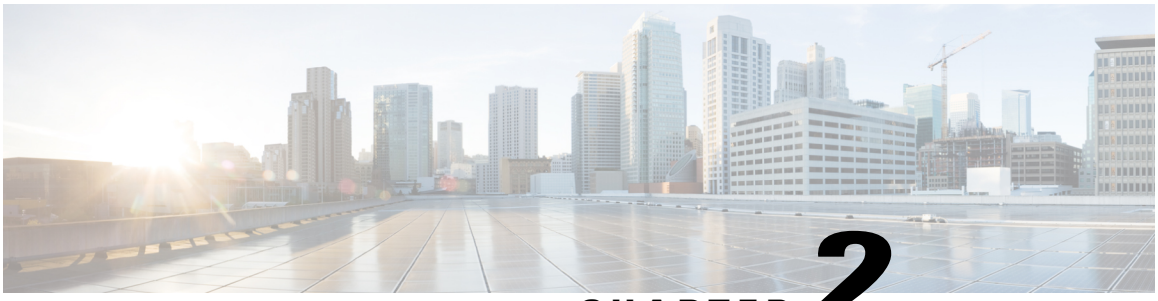
1. To increase or decrease the height of either of the left or right bottom pane, click the pane resize grippers at the top of the pane, then drag up or down with your mouse.
2. To collapse either the lower right or lower left pane, hover over the pane resize grippers at the top of the pane until a double-ended arrow is displayed, then click your mouse once.
3. To restore a collapsed pane, hover over the pane resize grippers at the bottom of the pane until a double-ended arrow is displayed, then click your mouse once.
4. To increase or decrease the width of the two left panes at the same time, click the pane resize grippers at the top of the pane, then drag left or right with your mouse.

Saving Configuration Changes

You should periodically save the configuration changes that you make in Cisco Monitor Manager.

Note Any unsaved configuration changes in Cisco Monitor Manager will be lost if you stop the Cisco XNC application.

On the Cisco Monitor Manager menu bar, click **Save**.



CHAPTER 2

Configuring Ports and Devices

This chapter contains the following sections:

Cisco Monitor Manager Port Types

Cisco Monitor Manager allows you to configure different port types. All configured ports are displayed in the **Configured Ports** table on the **Port Types** tab.

Edge Ports

Edge ports are the ingress ports where traffic enters the monitor network. Cisco Monitor Manager supports the following edge ports:

- TAP ports—An edge port for incoming traffic connected to a physical tap wire.
- SPAN ports—An edge port for incoming traffic connected to an upstream switch that is configured as a SPAN destination.

Configuring an edge port is optional.

Delivery Ports

Delivery ports are the egress ports where the traffic exits the monitor network. These outgoing ports are connected to a external monitoring device. When you configure a monitor device in Cisco Monitor Manager, you can associate a name and an icon with the switch and port that you configured.

Configured devices are displayed in the **Monitor Devices** table on the **Devices** tab. The icon appears in the topology diagram with a line connecting it to the node.

VLAN Double Tagging

Cisco Monitor Manager allows you to configure a switch port as an edge port and specify a VLAN for that port. When this is done, Cisco Monitor Manager programs the Cisco Nexus 3000 or 3100 Series switch so that all packets received in that port are VLAN tagged, and the VLAN ID is the one configured on the edge port. If the packets received in that port are already VLAN tagged frames, they will be double-tagged, and the outermost VLAN tag will contain the VLAN ID associated with the configured edge port.

Configuring a Port Type

DETAILED STEPS

	Command or Action	Purpose
Step 1	In the topology diagram, click the node for which you want to configure a port.	The **Port Types** tab displays the list of ports available to configure for that node.
Step 2	In the list of ports for the node, click **Click to configure** under the port identifier of the port you want to configure.	
Step 3	Click the **Select a port type** drop-down list.	
Step 4	Click one of the following: • **Edge Port-SPAN** • **Edge Port-TAP**	**Edge Port-SPAN—**Creates an edge port for incoming traffic connected to an upstream switch that is configured as a SPAN destination. **Edge Port-TAP—**Creates an edge port for incoming traffic connected to a physical TAP port.
Step 5	Enter a **Port Description**.	(Optional) The **Port Description** may contain between 1 and 256 alphanumeric characters including the following special characters: underscore (_), hyphen (-), plus (+), equals (=), open parenthesis ("("), closed parenthesis (")"), vertical bar (|), or at sign (@).
Step 6	Enter a **VLAN ID**.	(Optional) The port will be configured as dot1q to preserve any production VLAN information.
Step 7	Click **Submit**.	The port type configuration is saved and displayed in the description of the port under the node identifier.

Removing a Port Type Configuration

Step 1 In the topology diagram, click the node for which you want to remove a port configuration.
The **Port Types** tab displays the list of ports available to configure for that node.

Step 2 In the list of ports for the node, click the identifier of the port for which you want to remove the configuration.

Step 3 Click the **Edge Port-SPAN** or **Edge Port-Tap** link in the left pane.
The link displayed depends on the type of port that was configured.

Step 4 Click **Remove Configuration** from the drop-down list.
The port type configuration is removed.

Configuring a Monitor Device

Step 1 In the topology diagram, click the node for which you want to configure a monitoring device.
The **Port Types** tab displays the list of ports available to configure for that node.

Step 2 In the list of ports for the node, click **Click to configure** under the port identifier of the port you want to configure.

Step 3 Click **Add Monitoring Device**.

Step 4 In the **Add Device** dialog box, complete the following fields:

Name	Description
Device Name field	The name you want to use for the monitoring device. The name may contain between 1 and 256 alphanumeric characters including the following special characters: underscore (_), hyphen (-), plus (+), equals (=), open parenthesis ("("), closed parenthesis (")"), vertical bar (|), or at sign (@).
Icons selection	The choice of icons, with the first one selected by default. Choose any icon to use for the monitoring device.

Step 5 Click **Submit**.

Removing a Monitoring Device

Before You Begin

At least one monitoring device must be configured for the port.

Step 1 In the topology diagram, select the node from which you want to remove a monitoring device.

Step 2 Next to the port name for which you want to remove monitoring devices, click the **Devices** highlight.

Step 3 In the expanded **Device Name** list for the port, click either:

- The top checkbox to select all monitoring devices for removal
- The checkbox next to the name of only the monitoring device or devices you want to remove

Step 4 Click **Remove Monitoring Devices** above the **Device Name** list.

Step 5 In the confirmation dialog box, click **Remove Devices.**

Configuring a Root Node

A root node is automatically selected by Cisco Monitor Manager. If the defined root node is too far from the source switches, you can manually configure a different switch. We recommend that you choose a switch with edge ports as your new root node.

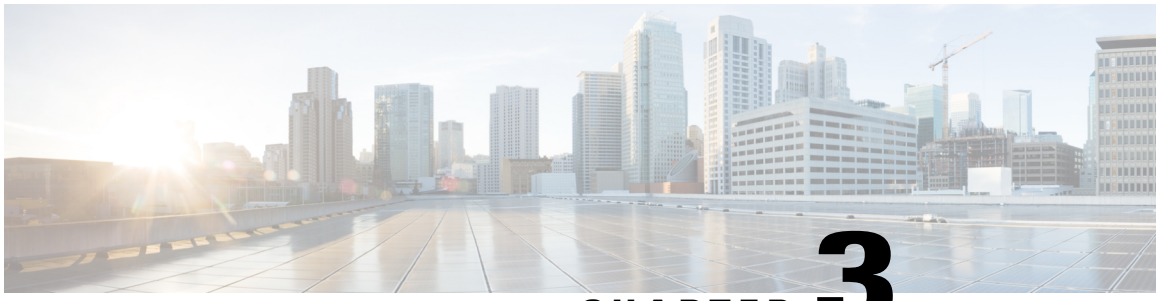
Note Root node changes do not take effect until you save the configuration and restart the Cisco XNC application.

Step 1 On the **Root** tab, click **Configure Root**.

Step 2 In the **Configure Root Node** dialog box, choose a node in the **Select Root Node** drop-down list.

Step 3 Click **Configure**.

Step 4 Restart Cisco Monitor Manager.



CHAPTER 3

Filtering Flows

This chapter contains the following sections:

Cisco Monitor Manager Networks

A Cisco Monitor Manager network consists of one or more Cisco Nexus 3000 Series switches with Cisco Plug-in for OpenFlow dedicated for connecting multiple spanned ports and network taps from the production network infrastructure. Cisco XNC programs the switches using the OpenFlow protocol. Cisco Monitor Manager filters the packets that travel the network and delivers them to a pool of connected monitoring devices.

Cisco Monitor Manager Forwarding Path Options

Cisco Monitor Manager supports the following forwarding path options:

Multipoint-to-Multipoint

With the Multipoint-to-Multipoint (MP2MP) forwarding path option, both the ingress edge port where SPAN or TAP traffic is coming in to the monitor network and the egress delivery ports are defined. Cisco Monitor Manager uses the delivery ports to direct traffic from that ingress port to one or more devices.

Any-to-Multipoint

With the Any-to-Multipoint (A2MP) forwarding path option, the ingress edge port of the monitor network is not known, but the egress delivery ports are defined. Cisco Monitor Manager automatically calculates a loop-free forwarding path from the root node to all other nodes using the Single Source Shortest Path (SSSP) algorithm.

Cisco Monitor Manager Filters and Rules

Filters

You can use a filter to define the Layer 2 (L2), Layer 3 (L3), and Layer 4 (L4) criteria used by Cisco Monitor Manager to filter traffic. Traffic that matches the criteria in the filter is routed to the delivery ports and from there to the attached monitor devices.

Rules

You can use rules to associate filters to configured monitor devices. You can configure rules with or without a source. Rules with a source node and port use the Multipoint-to-Multipoint forwarding path option. Rules without a source port on a node use the loop-free Any-to-Multipoint forwarding path option.

Each rule has a priority that can be configured. Flows with a higher priority are given precedence over flows with a lower priority.

Adding a Filter

Note The priority you want to set was moved from filters to rules in Cisco XNC Release 1.5. If you upgraded from Cisco XNC Release 1.0 to Cisco XNC Release 1.5, any filters and rules that you previously configured in Cisco Monitor Manager 1.0 will automatically be converted to the new format in Cisco Monitor Manager 1.5.

Step 1 In the **Configure Filters** tab, click **Add Filter**.

Step 2 In the **Filter Description** section of the **Add Filter** dialog box, complete the following fields:

Name	Description
Name field	The name of the filter. The name may contain between 1 and 256 alphanumeric characters including the following special characters: underscore (_), hyphen (-), plus (+), equals (=), open parenthesis ("("), closed parenthesis (")"), vertical bar (|), or at sign (@). The name cannot be changed once you have saved it.

Name	Description
Bidirectional checkbox	Check this box if you want the filter to capture traffic information from a source IP, source port, or source MAC to a destination IP, destination port, or destination MAC, and from a destination IP, destination port, or destination MAC to a source IP, source port, or source MAC.

Step 3 In the **Layer 2** section of the **Add Filter** dialog box, complete the following fields:

Name	Description
Ethernet Type drop-down list	Required. The Ethernet type of the Layer 2 traffic. The default value displayed is IPv4, or you can choose one of the following: • **IPv6** • **ARP** • **LLDP** • **Enter Ethernet Type** If you choose **Enter Ethernet Type** as the type, enter the Ethernet type in hexadecimal format.
VLAN Identification Number field	The VLAN ID for the Layer 2 traffic.
VLAN Priority field	The VLAN priority for the Layer 2 traffic.
Source MAC Address field	The source MAC address of the Layer 2 traffic.
Destination MAC Address field	The destination MAC address of the Layer 2 traffic.

Step 4 In the **Layer 3** section of the **Add Filter** dialog box, complete the following fields:

Name	Description
Source IP Address field	The source IP address of the Layer 3 traffic. This can be one of the following: • The host IP address, for example, 10.10.10.10 • An IPv4 address range, for example, 10.10.10.10-10.10.10.15 • The host IP address in IPv6 format, for example, 2001::0 **Note** You cannot enter a range of IPv6 addresses for the **Source IP Address**.

Name	Description
Destination IP Address field	The destination IP address of the Layer 3 traffic. This can be one of the following: • The destination IP address. For example, 10.10.10.11 • An IPv4 address range, for example, 10.10.11.10-10.10.11.15 • The destination IP address in IPv6 format, for example, 2001::4 **Note** You cannot enter a range of IPv6 addresses for the **Destination IP Address**.
Protocol drop-down list	The Internet protocol of the Layer 3 traffic. This can be one of the following: • **ICMP** • **TCP** • **UDP** • **Enter Protocol** If you choose **Enter Protocol** as the type, enter the protocol number in decimal format.
ToS Bits field	The Type of Service (ToS) bits in the IP header of the Layer 3 traffic. Only the Differentiated Services Code Point (DSCP) values are used.

Step 5 In the **Layer 4** section of the **Add Filter** dialog box, complete the following fields:

Name	Description
Source Port drop-down list	The source port of the Layer 4 traffic. Choose one of the following: • **FTP (Data)** • **FTP (Control)** • **SSH** • **TELNET** • **HTTP** • **HTTPS** • **Enter Source Port** If you choose Enter Source Port, enter the source port number.
Destination Port drop-down list	The destination port of the Layer 4 traffic. Choose one of the following: • **FTP (Data)** • **FTP (Control)** • **SSH** • **TELNET** • **HTTP** • **HTTPS** • **Enter Destination Port** If you choose Enter Destination Port, enter the destination port number.

Step 6 Click **Add Filter**.

Editing a Filter

Before You Begin

You must have added a filter before you can edit it.

Note You cannot change the filter **Name** and you cannot edit the **Layer 4** section fields in the **Edit Filter** dialog box.

Step 1 In the **Configure Filters** tab, click **Edit Filter** button next to the **Name** of the filter you want to edit.

Step 2 In the **Edit Filter** dialog box, edit the following fields:

Name	Description
Name field	The name of the filter. The name may contain between 1 and 256 alphanumeric characters including the following special characters: underscore (_), hyphen (-), plus (+), equals (=), open parenthesis ("("), closed parenthesis (")"), vertical bar (|), or at sign (@). The name cannot be changed once you have saved it.
Bidirectional checkbox	Check this box if you want the filter to capture traffic information from a source IP, source port, or source MAC to a destination IP, destination port, or destination MAC, and from a destination IP, destination port, or destination MAC to a source IP, source port, or source MAC.

Step 3 In the **Layer 2** section of the **Edit Filter** dialog box, edit the following fields:

Name	Description
Ethernet Type drop-down list	Required. The Ethernet type of the Layer 2 traffic. The default value displayed is IPv4, or you can choose one of the following: • **IPv6** • **ARP** • **LLDP** • **Enter Ethernet Type** If you choose **Enter Ethernet Type** as the type, enter the Ethernet type in hexadecimal format.
VLAN Identification Number field	The VLAN ID for the Layer 2 traffic.
VLAN Priority field	The VLAN priority for the Layer 2 traffic.
Source MAC Address field	The source MAC address of the Layer 2 traffic.

Name	Description
Destination MAC Address field	The destination MAC address of the Layer 2 traffic.

Step 4 In the **Layer 3** section of the **Edit Filter** dialog box, edit the following fields:

Name	Description
Source IP Address field	The source IP address of the Layer 3 traffic. This can be one of the following: • The host IP address, for example, 10.10.10.10 • An IPv4 address range, for example, 10.10.10.10-10.10.10.15 • The host IP address in IPv6 format, for example, 2001::0 **Note** You cannot enter a range of IPv6 addresses for the **Source IP Address**.
Destination IP Address field	The destination IP address of the Layer 3 traffic. This can be one of the following: • The destination IP address. For example, 10.10.10.11 • An IPv4 address range, for example, 10.10.11.10-10.10.11.15 • The destination IP address in IPv6 format, for example, 2001::4 **Note** You cannot enter a range of IPv6 addresses for the **Destination IP Address**.
Protocol drop-down list	The Internet protocol of the Layer 3 traffic. This can be one of the following: • **ICMP** • **TCP** • **UDP** • **Enter Protocol** If you choose **Enter Protocol** as the type, enter the protocol number in decimal format.
ToS Bits field	The Type of Service (ToS) bits in the IP header of the Layer 3 traffic. Only the Differentiated Services Code Point (DSCP) values are used.

Deleting a Filter

You can delete filters that are associated with rules and the rules are deleted at the same time.

Step 1 On the **Configure Filters** tab, click the checkbox next to filter or filters that you want to delete, then click **Remove Filters**.
When filters have rules associated with them, this information is displayed in the **Remove Filters** dialog box.

Step 2 In the **Remove Filters** dialog box, click **Remove Filters**.

Adding a Rule

Before You Begin

- Configure a monitoring device.
- Add a filter to be assigned to the rule.
- Optional: Configure an edge port or multiple edge ports.

Step 1 On the **Apply Filters** tab, click the Edit button next to the **Add Rule**.

Step 2 In the **Add Rule** dialog box, complete the following fields:

Field	Description
Rule Name field	The name of the rule. The name may contain between 1 and 256 alphanumeric characters including the following special characters: underscore (_), hyphen (-), plus (+), equals (=), open parenthesis ("("), closed parenthesis (")"), vertical bar (|), or at sign (@).
Rule Filter drop-down list	Choose the filter that you want to assign to the rule.
Priority field	The priority you want to set for the rule. The default is 100, and the valid range of values is 0 through 10000.
Set VLAN field	The VLAN ID you want to set for the rule.

Field	Description
Deny all matching traffic checkbox	Check this box if you want to drop all traffic based on the filter. **Note** If deny all matching traffic is checked, you will be unable to select destination monitoring devices.
Destination Devices field	The monitoring devices that you want to associate with the filter. You can choose one or more devices.
Select Source Node drop-down list	Choose the source node that you want to assign. **Note** If you do not choose a source node, the Any-to-Multipoint loop-free forwarding path option is used, and traffic from all non-delivery ports is evaluated against the filter.
Select Source Port drop-down list	Choose the port on the source node that you want to assign. **Note** Only edge ports can be used as source ports.

Step 3 Click **Submit**.

Viewing and Modifying Rules

After you have created a rule, you can modify the devices associated with the rule or delete the rule.

Step 1 Navigate to the **Apply Filters** tab.

Step 2 The **Rules** table displays the following information for each rule:

Field	Description
Rule Name field	The name that you assigned to the rule.
Filter Name field	The filter that you assigned to the rule.
Port Name field	The source port that you assigned to the rule, if any.
Switch Name field	The source node that you assigned to the rule, if any.
Devices field	The monitor devices that are associated with the filter.
Created by field	The name and role of the user who created the rule.

Step 3 Click a rule to view the forwarding path for that rule in the topology diagram.
The path is highlighted in red.

Step 4 Click the **Edit** button to modify a rule.

Step 5 In the **Modify Rule** dialog box, perform one of the following tasks:

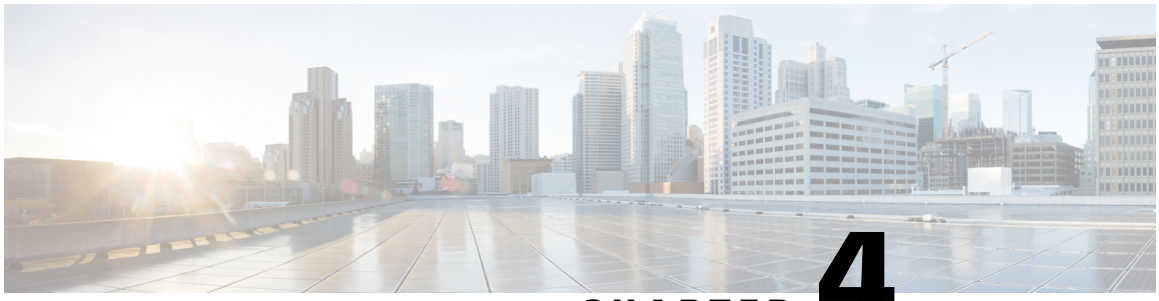
- Add or remove devices and click **Submit**.
- Click **Remove Rule** to delete the rule.
- Click **Close** to close the dialog box without making any changes.

Deleting a Rule

Step 1 Navigate to the **Apply Filters** tab.

Step 2 Click the check box for the rule or rules that you want to delete.

Step 3 Click **Remove Rules**.



CHAPTER 4

Managing Users

This chapter contains the following sections:

Cisco Monitor Manager Users

Cisco Monitor Manager uses roles and levels to manage user access. One of the following levels can be assigned to each role that you create:

- **App-Administrator—**Has full access to all Cisco Monitor Manager resources.
- **App-User—**Has full access to resources that are assigned to his resource group and resources that are created by another user who has similar permissions.

Each role is assigned one or more groups, which are collections of resources. Group resources are non-ISL ports that are specifically assigned to that group. After you have created a group, you can assign that group to a role.

For information about AAA integration, see the *Cisco Extensible Network Controller Configuration Guide*.

Creating a Role

Step 1 On the **Admin** drop-down list, choose **Settings**.

Step 2 On the **Roles** tab, click **Add Role**.

Step 3 In the **Add Role** dialog box, complete the following fields:

Field	Description
Name field	The name of the role. The name may contain between 1 and 256 alphanumeric characters including the following special characters: underscore (_), hyphen (-), plus (+), equals (=), open parenthesis ("("), closed parenthesis (")"), vertical bar (|), or at sign (@).
Level drop-down list	Choose the level that you want to assign to the role. This can be one of the following: • **App-Administrator—**Has full access to all Cisco Monitor Manager resources. • **App-User—**Has full access to resources that are assigned to his resource group and resources that are created by another user who has similar permissions.

Step 4 Click **Submit**.

Configuring a Role to Access Multiple Disjoint Networks

Roles can be configured to permit role-based access to multiple Cisco Monitor Manager disjoint networks.

For example, if you have two networks, the first named **eng** and the second named **hr1**, the network administrator can create a Cisco Monitor Manager role that has access to both networks. The access level for network **eng** can be assigned as **App-Admin**, and the access level for network **hr1** can be assigned as **App-User**.

The steps below provide a guide to creating an example role named “MM-role-eng-hr1” that will have access to multiple Cisco Monitor Manager disjoint networks.

Note Do not enter the quotation marks (" ") used in the example steps.

Step 1 Log in to the first Cisco Monitor Manager network, in this example, **eng**, with the App-Administrator role user name and password.

Step 2 On the menu bar, choose **Settings** from the **Admin** drop-down list .

Step 3 Click **Add Role**.

Step 4 In the **Name** field of the **Add Role** dialog box, enter a name for the role, for example, “MM-role-eng-hr1”.
The name may contain between 1 and 256 alphanumeric characters including the following special characters: underscore (_), hyphen (-), plus (+), equals (=), open parenthesis ("("), closed parenthesis (")"), vertical bar (|), or at sign (@).

Step 5 From the **Level** drop-down list, choose **App-Administrator**.

Step 6 Click **Submit**.

Step 7 From the menu bar, choose network **hr1** from the network drop-down, or log in to network **hr1** with the App-Administrator role name and password.

Step 8 Repeat Steps 2 and 3.

Step 9 In the **Name** field of the **Add Role** dialog box, enter the same name for the role that you entered in Step 4.

Step 10 From the **Level** drop-down list, choose **App-User**.

Step 11 Click **Submit**.
The role “MM-role-eng-hr1” now has App-Administrator permissions to network **eng** and App-User permissions to network **hr1**.

Removing a Role

Note You cannot remove roles that were created by Cisco XNC

Step 1 On the **Admin** drop-down list, choose **Settings**.

Step 2 In the **Roles** table on the **Roles** tab, click the role that you want to remove.

Step 3 In the **Remove Roles** dialog box, click **Remove**.

Creating a Resource Group

Step 1 On the **Admin** drop-down list, choose **Settings**.

Step 2 On the **Groups** tab, click **Add Group**.

Step 3 In the **Add Resource Group** dialog box, enter the name that you want to use for the resource group.
The name may contain between 1 and 256 alphanumeric characters including the following special characters: underscore (_), hyphen (-), plus (+), equals (=), open parenthesis ("("), closed parenthesis (")"), vertical bar (|), or at sign (@).

Step 4 Click **Submit**.

What to Do Next

Assign resources to the group.

Adding Resources to a Resource Group

Before You Begin

Create a group.

Step 1 On the **Admin** drop-down list, choose **Settings**.

Step 2 On the **Groups** tab, choose the group to which you want to add resources.

Step 3 Choose a node in the topology diagram.

Step 4 In the **Add Ports to Group** dialog box, choose the ports that you want to add to the group.

Step 5 Click **Submit**.

Step 6 Repeat Step 3 through Step 5 for all of the ports that you want to add.

Step 7 To remove a resource, choose one or more ports in the **Group Detail** table, and then click **Remove Ports**.

Step 8 In the **Remove Ports** dialog box, click **Remove**.

What to Do Next

Assign the group to a role.

Removing a Group

The following groups cannot be removed:

- The default **allPorts** group

- Any group that has been assigned to a role.

Step 1 On the **Admin** drop-down list, choose **Settings**.
Step 2 On the **Groups** tab, choose the group or groups that you want to remove.
Step 3 Click **Remove Groups**.
Step 4 In the **Remove Resource Groups** dialog box, click **Remove**.

Assigning a Group to a Role

Before You Begin

- Create a role.
- Create a group.

Step 1 On the **Admin** drop-down list, choose **Settings**.
Step 2 Choose the **Assign** tab.
Step 3 Click **Assign** next to the role for which you want to assign a group.
Step 4 In the **Configure Role** dialog box, complete the following fields:

Field	Description
Assign Group field	Choose the groups that you want to assign to the role. You can choose one or more groups to assign. **Note** You cannot assign a group to a role with the App-Administrator level.
Unassign Group field	Choose the groups that you want to unassign from the role. You can choose one or more groups to unassign. **Note** You cannot unassign the allPorts group from a role with the App-Administrator level.

Step 5 Click **Apply**.

Unassigning a Group

Step 1 On the **Admin** drop-down list, choose **Settings**.

Step 2 Choose the **Assign** tab.

Step 3 Click **Assign** next to the role for which you want to unassign a group.

Step 4 In the **Configure Role** dialog box, choose a port in the **Unassign Group** drop-down list.

Step 5 Click **Apply**.