Cisco Monitor Manager Application Configuration Guide, Release 1.6

First Published: June 11, 2014

Last Modified: July 25, 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-32190-01

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:

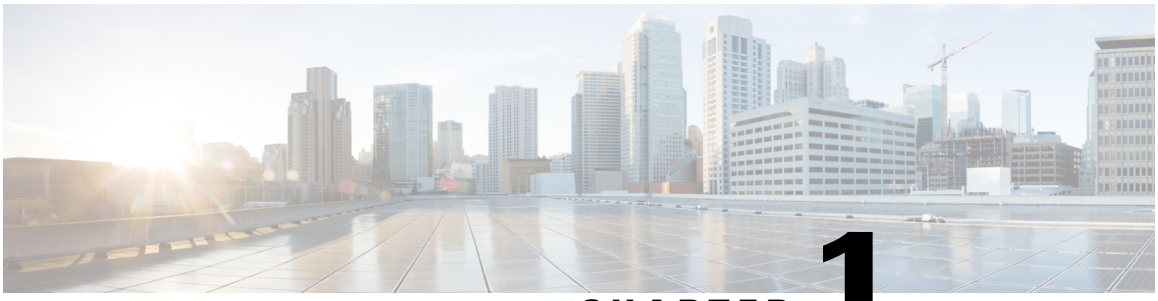
Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

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/c/en/us/td/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 (XNC) is a software platform that serves as an interface between the network elements (southbound) and third-party applications (northbound). Cisco XNC, which is a JVM-based application that runs on a Java Virtual Machine (JVM), is based on a highly available, scalable, and extensible architecture. Cisco XNC is built for extensibility using the Open Services Gateway initiative (OSGi) framework.

Cisco XNC can support multiple protocol plugins in the southbound direction. In Release 1.6, Cisco Plug-in for OpenFlow 1.0 and the Cisco One Platform Kit (onePK) are supported.

Cisco XNC provides the following:

- Multiprotocol capability with the Cisco Plug-in for OpenFlow.
- 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 Cisco Monitor Manager, which 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 Release 1.6 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 command line interface (CLI) framework for Cisco XNC.
- The Virtual Patch Panel Application (Port-to-Port Forwarding application) provides port-to-port traffic management within a switch or across the network without any need for physical connection changes or rewiring.
- Access to the Cisco XNC northbound API content from the application menu bar that enables you to view the API definitions and related calls.

About Cisco Monitor Manager

Cisco Monitor Manager is a network application that runs on Cisco Extensible Network Controller (XNC). Cisco Monitor Manager, in combination with the Cisco Plug-in for OpenFlow and Cisco Nexus 3000 or 3100 Series switchs, 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 Cisco 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 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.
- Connect to Cisco onePK agents for which Cisco onePK devices have been configured in Cisco XNC.
- Set VLAN is supported on Cisco Nexus 3000 and 3100 Series switches.
- Configure symmetric load balancing or QinQ, depending on whether the network device is a Cisco Nexus 3000 or 3100 Series switch:
    - Symmetric Load Balancing is supported on Cisco Nexus 3100 Series switches.
    - QinQ is supported on Cisco Nexus 3000 and 3100 Series switches.

Configuring User Roles for Edge Ports

To manage which edge ports a Cisco Monitor Manager application user can use for creating rules for edge ports, you must modify the App-User role settings in the config.ini file to enable role-based access control (RBAC) for application users. After you make your changes and restart Cisco Extensible Network Controller (XNC), note these restrictions:

- Cisco Monitor Manager App-User role users will be able to create rules only for source ports which are part of the resource group or groups assigned to that role .
- 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 false).`

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 Extensible Network Controller (XNC) is running, restart the application to enable the change.

Logging in to the Cisco Monitor Manager GUI

You must log into the Cisco Monitor Manager using HTTPS. 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 **Online help** button—Provides access to the online help for the current page.
- A **Save** button—Enables you to save any additions or changes you make in the Cisco Monitor Manager application.
- A **Northbound API** button—Enables you to view northbound API content in a new browser tab, and displays the content and calls.
- The administrative management (**Admin**) drop-down list—Provides access to different administrative tasks, such as managing roles and resource groups.

Note The **Admin** drop-down list—Displays the username that you used when you logged into Cisco Monitor Manager.

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 as follows:

- Move mode—Moves 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—Increases 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—Decreases 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—Zooms in on a specific topology element. To zoom by selection, click the tool, then click and drag your mouse across the element that you want to zoom in on. The zoom element display resets after a few seconds.
- Fit stage—Resets the topology diagram in the topology pane.
- Topology Settings—Choose the preferred **Display Icons as dots** setting. Click the radio button for the preference that you desire.
- 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 as follows:

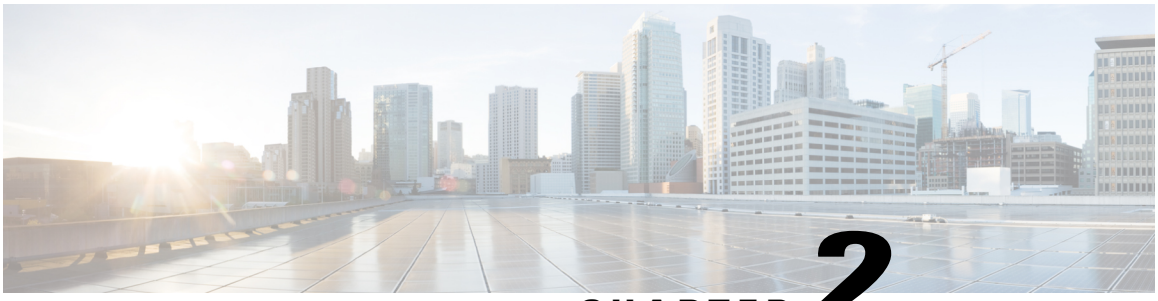
- To increase or decrease the height of either of the left or right bottom pane, click the pane resize grippers at the top of the pane, and then drag up or down with your mouse.
- To collapse either the lower right or lower left pane, hover over the pane resize grippers at the top of the pane until a double-ended arrow is displayed, and then click your mouse once.
- To restore a collapsed pane, hover over the pane resize grippers at the bottom of the pane until a double-ended arrow is displayed, and then click your mouse once.
- 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, and 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 Extensible Network Controller (XNC) application.

On the menu bar, click **Save**.



CHAPTER 2

Configuring Ports and Devices

This chapter contains the following sections:

About Cisco Monitor Manager Port Types

Cisco Monitor Manager enables 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—For incoming traffic connected to a physical tap wire.
- SPAN ports—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 external monitoring devices. When you configure a monitoring 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 that connects it to the node.

VLAN Double Tagging

Cisco Monitor Manager enables you to configure a switch port as an edge port and specify a VLAN for that port. When you configure the VLAN ID, and the connection to the Cisco onePK agent is up, 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 get double-tagged, and the outermost VLAN tag contains the VLAN ID that is associated with the configured edge port.

Configuring a Port Type

Step 1 In the topology diagram, click the node for which you want to configure a port.
The **Ports** area of the sidebar 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 that you want to configure.

Step 3 From the **Select a port type** drop-down list, choose 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 4 (Optional) In the **Port Description** field, enter a port description.
The port description can contain between 1 and 256 alphanumeric characters, including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").

Step 5 (Optional) Enter a VLAN ID.
The port is configured as dot1q to preserve any production VLAN information.

Step 6 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 In the left pane, click the **Edge Port-SPAN** or **Edge Port-TAP** link.
The link displayed depends on the type of port that was configured.

Step 4 From the drop-down list, choose **Remove Configuration**.
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 that 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. You can edit the name of the monitoring device after it has been added. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), 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. You can edit the monitoring device icon after the monitoring device has been added.

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, choose 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, choose one of the following:

- 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 Above the **Device Name** list, click **Remove Monitoring Devices**.

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 Extensible Network Controller (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.

Cisco onePK Agent

The Cisco onePK plug-in for Cisco Extensible Network Controller (XNC) communicates with onePK devices through a onePK agent on the device. To support onePK device functions in Cisco Monitor Manager, the application must be connected to the onePK agent. The agent is the mediator between Cisco Monitor Manager and onePK-enabled devices that are configured in Cisco Extensible Network Controller (XNC).

To secure communication between Cisco Extensible Network Controller (XNC) onePK-enabled devices, you must configure Transport Layer Security (TLS) in Cisco Extensible Network Controller (XNC). See the *Cisco Extensible Network Controller Deployment Guide, Release 1.6* for detailed procedures.

Connecting to a onePK Agent

You must connect to a onePK agent to support additional functionality in Cisco Monitor Manager, including symmetric load balancing and Q-in-Q.

Step 1 In the topology diagram, click the node to which you wish to connect a onePK agent.

Step 2 In the sidebar, click **Click to enable addtional functionality**.

Step 3 In the **Connect to onePK agent** dialog box, complete the following fields:

Name	Description
Address field	The IP address assigned to the Cisco onePK device.
Username field	The username of the user that you want to assign to the device.
Password field	The password of the user that you want to assign to the device.

Step 4 Click **Submit**.

Symmetric Load Balancing

Cisco Monitor Manager enables you to configure symmetric load balancing settings on the egress port channels. Load balancing settings are based on Layer 2 source MAC and destination IP addresses, or Layer 2, Layer 3, or Layer 4 source and destination ports. When you configure symmetric load balancing for all the port-channel interfaces on the switch, all the traffic from specific sources and destinations in both directions always flows on the same port-channel member link.

Note Symmetric load balancing in Cisco Monitor Manager is available only for Cisco Nexus 3100 Series switches.

Configuring Symmetric Load Balancing

Note The ability to configure symmetric load balancing is available only for Cisco Nexus 3100 Series switches.

Before You Begin

- Configure a onePK agent for the node.
- Configure and provision TLS on the switches. See the *Cisco Extensible Network Controller Deployment Guide, Release 1.6* for detailed TLS setup procedures.

Step 1 In the topology diagram, click the node for which you wish to configure symmetric load balancing.

Step 2 In the side bar, from the **Symmetric Load Balancing** drop-down list, choose one of the following:

- **SOURCE_DESTINATION_IP—**source and destination IP address (includes Layer 2)
- **SOURCE_DESTINATION_IP_ONLY—**source and destination IP addresses only
- **SOURCE_DESTINATION_PORT—**source and destination TCP/UDP port (includes Layer 2 and Layer 3)
- **SOURCE_DESTINATION_PORT_ONLY—**source and destination TCP/UDP port only

Step 3 Click **Submit**.

Configuring Q-in-Q

Note The ability to configure Q-in-Q is available only for Cisco Nexus 3000 and 3100 Series switches. Q-in-Q is automatically enabled when you configure a VLAN ID for an edge port, if the VLAN ID is maintained on the edge port.

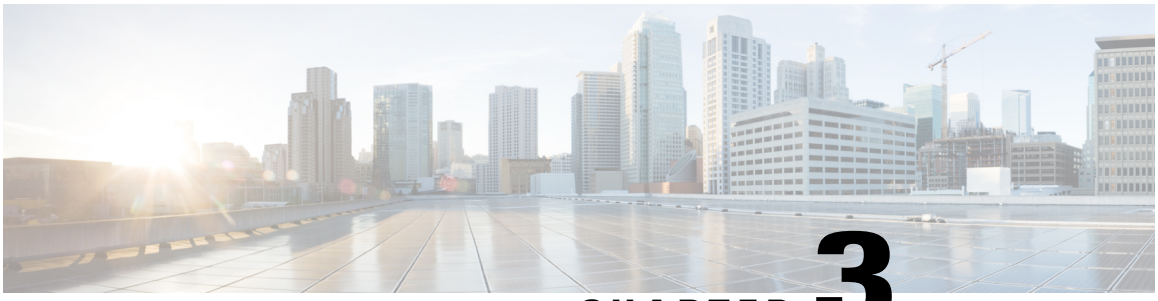
Before You Begin

Connect to the onePK agent for the node.

Step 1 In the topology diagram, click the node for which you wish to configure Q-in-Q.

Step 2 In the side bar, configure an edge port and set a VLAN ID on that edge port.

Step 3 Click **Submit**.



CHAPTER 3

Filtering Flows

This chapter contains the following sections:

About Cisco Monitor Manager Networks

A Cisco Monitor Manager network consists of one or more Cisco Nexus 3000 and 3100 Series switches with Cisco Plug-in for OpenFlow dedicated for connecting multiple spanned ports and network taps from the production network infrastructure. Cisco Extensible Network Controller (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.

About 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 into the monitor network and the egress delivery ports are defined. Cisco Monitor Manager uses the delivery ports to direct traffic from those ingress ports 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.

About Filters and Rules

Filters

In Cisco Monitor Manager, you can use a filter to define the Layer 2 (L2), Layer 3 (L3), and Layer 4 (L4) criteria used 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.

When a rule is configured with the Deny option, the ingress edge ports may or may not be defined. Cisco Monitor Manager drops traffic on the specified ingress edge port(s) or on all nodes if no ingress edge ports are defined.

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

Rules can be created and saved without installing them. After they are saved, installation can be toggled on and off in the Cisco Monitor Manager GUI.

Adding a Filter

Note The priority setting was moved from filters to rules in Cisco Extensible Network Controller (XNC) Release 1.5. If you upgraded from Cisco Extensible Network Controller (XNC) Release 1.0 to Cisco Extensible Network Controller (XNC) Release 1.5, any filters and rules that you previously configured in Cisco Monitor Manager 1.0 are automatically converted to the new format in Cisco Monitor Manager, Release 1.5.

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

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

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 in the **Source IP Address** field. • If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 4 source or destination ports.

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 in the **Destination IP Address** field. • If you configure a range of Layer 3 destination IP addresses, you cannot configure ranges of Layer 4 source or destination ports.
Protocol drop-down list	Choose 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	Choose the source port of the Layer 4 traffic. This can be one of the following: • **FTP (Data)** • **FTP (Control)** • **SSH** • **TELNET** • **HTTP** • **HTTPS** • **Enter Source Port** If you choose **Enter Source Port**, enter either a single port number or a range of source port numbers. **Note** If you configure a range of Layer 4 source ports, you cannot configure ranges of Layer 3 IP source or destination addresses.
Destination Port drop-down list	Choose the destination port of the Layer 4 traffic. This can be one of the following: • **FTP (Data)** • **FTP (Control)** • **SSH** • **TELNET** • **HTTP** • **HTTPS** • **Enter Destination Port** If you choose **Enter Destination Port**, enter either a single port number or a range of destination port numbers. **Note** If you configure a range of Layer 4 destination ports, you cannot configure ranges of Layer 3 IP source or destination addresses.

Step 6 Click **Add Filter**.

Editing a Filter

Before You Begin

You must add a filter before you can edit it.

Note You cannot change the filter **Name** in the **Edit Filter** dialog box.

Step 1 On the **Configure Filters** tab, click the **Edit** button next to the **Name** of the filter that 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 can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@"). **Note** The name cannot be changed once you have saved it.
Bidirectional check box	Check this box if you want the filter to capture traffic information from a source IP, source port, or source MAC address to a destination IP, destination port, or destination MAC address, and from a destination IP, destination port, or destination MAC to a source IP, source port, or source MAC address.

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

Name	Description
Ethernet Type field	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** • **Predefined EtherTypes** • **Enter Ethernet Type** If you choose **Enter Ethernet Type** as the type, enter the Ethernet type in hexadecimal format. If you choose **Predefined EtherTypes**, all predefined Ethernet types contained in the config.ini file are associated with the rule, and you should not configure any other parameters. **Note** If you do configure any other parameters along with **Predefined EtherTypes**, then click **Save Rule**, an error message will be displayed.
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 **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 in the **Source IP Address** field. • If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 4 source or destination ports.
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 in the **Destination IP Address** field. • If you configure a range of Layer 3 destination IP addresses, you cannot configure ranges of Layer 4 source or destination ports.
Protocol drop-down list	Choose 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.

Name	Description
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 a filter that has associated rules, resulting in removal of all the rules at the same time.

Step 1 On the **Configure Filters** tab, check the check box next to filter or filters that you want to delete, and 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

- Add a filter to be assigned to the rule.
- Configure a monitoring device (optional).
- Configure an edge port or multiple edge ports (optional).

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

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

Field	Description
Rule Name field	The name of the rule. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@"). **Note** The **Rule Name** cannot be modified after the rule is saved.
Rule Filter drop-down list	Choose the filter that you want to assign to the rule. **Note** The **Rule Filter** cannot be modified after the rule is saved.
Priority field	The priority that you want to set for the rule. The default is 100, and the valid range of values is 0 through 10000.

Step 3 In the **Actions** area, complete the following fields:

Field	Description
Set VLAN field	The VLAN ID that you want to set for the rule.
Strip VLAN at delivery port check box	Check this box to strip the VLAN tag from the packet before it reaches the delivery port. **Note** The **Strip VLAN at delivery port** action is only valid for rules with a single edge port and one or more delivery devices for a single, separate node.
Deny all matching traffic check box	Check this box if you want to drop all traffic based on the filter. **Note** If you check the **Deny all matching traffic** check box, you cannot select destination monitoring devices.
Destination Devices list	The monitoring devices that you want to associate with the filter. You can choose one or more devices by checking the boxes.

Step 4 (Optional) In the **Assign Source Ports** area, complete the following fields:

Field	Description
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 nondelivery 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 5 Do one of the following:

- Click **Save Rule** to save the rule, but not to install it until later.
- Click **Install Rule** to save the rule and install it at the same time.

Modifying a Rule

Note You cannot modify the **Rule Name** or **Rule Filter** in the **Modify Rule** dialog box.

Before You Begin

You must add the rule before you can modify it.

Step 1 On the **Apply Filters** tab, click the **Edit** button next to the **Name** of the rule that you want to modify.

Step 2 In the **Modify Rule** dialog bog you can modify the **Rule Priority** in the **Rule Details** area:

Field	Description
Rule Name field	The name of the rule. **Note** The **Rule Name** cannot be modified after the rule is saved.
Rule Filter drop-down list	The filter applied to the rule. **Note** The **Rule Filter** cannot be modified after the rule is saved.

Field	Description
Priority field	The priority that you want to set for the rule. The default is 100, and the valid range of values is 0 through 10000.

Step 3 In the **Actions** area, modify the following fields:

Field	Description
Set VLAN field	The VLAN ID that you want to set for the rule.
Strip VLAN at delivery port check box	Check this box to strip the VLAN tag from the packet before it reaches the delivery port. **Note** The **Strip VLAN at delivery port** action is only valid for rules with a single edge port and one or more delivery devices for a single, separate node.
Deny all matching traffic check box	Check this box if you want to drop all traffic based on the filter. **Note** If you check the **Deny all matching traffic** check box, you cannot select destination monitoring devices.
Destination Devices list	The monitoring devices that you want to associate with the filter. You can choose one or more devices by checking the boxes.

Step 4 In the **Assign Source Ports** area, complete the following fields:

Field	Description
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 nondelivery 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.

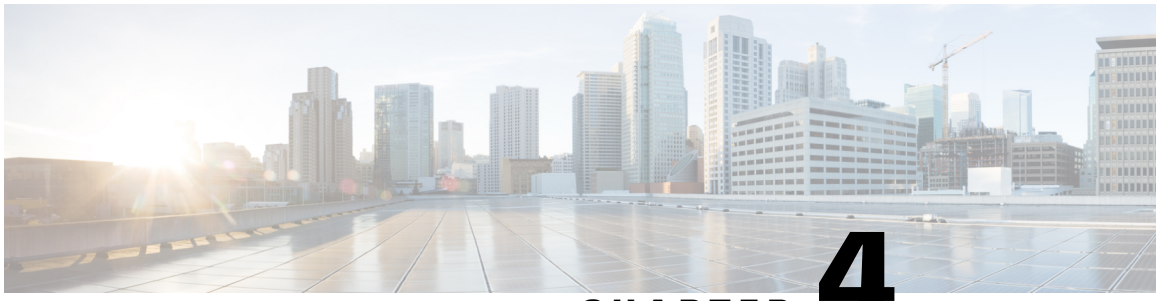
Step 5 Click **Submit**.

Deleting a Rule

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

Step 2 Check 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:

About 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 to one or more groups, which are collections of resources. Group resources are non-Inter Switch Link (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 In the menu bar, click the **Admin** drop-down list, and 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 can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), 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

Multiple disjoint networks are the virtual networks that you create using the Slice Manager in the Cisco Extensible Network Controller (XNC) application. 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 **dev** and the second named **prod**, the network administrator can create a user that has access to both networks but with difference privileges for each network. The access level for network **dev** can be assigned as **App-Admin**, and the access level for network **prod** can be assigned as **App-User**.

The App-Admin privilege provides the ability to create, edit, and delete his or other roles' rules and filters on the assigned network, in this case, dev. The App-User privilege provides the ability to create, edit, and delete rules and filters owned by this role only on the assigned network, in this case, prod. The application user role can create, edit, or delete rules and filters only for the disjoint network or networks to which the role has been

assigned. In addition, the application user role can view and apply filters created by the application administrator, but cannot edit or delete them.

Step 1 Log in to the Cisco Monitor Manager network with the Network-Admin role username and password.

Step 2 Ensure that you are in the **dev** network.

Step 3 On the menu bar, choose **Settings** from the **Admin** drop-down list .

Step 4 Click **Add Role**.

Step 5 In the **Name** field of the **Add Role** dialog box, enter the name for the role, for example, MM-role-dev.
The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").

Step 6 From the **Level** drop-down list, choose **App-Administrator**.

Step 7 Click **Submit**.

Step 8 On the menu bar, choose the **prod** network from the network drop-down list.

Step 9 Repeat Steps 3 and 4 for the **prod** network.

Step 10 In the **Name** field of the **Add Role** dialog box, enter MM-role-prod.

Step 11 From the **Level** drop-down list, choose **App-User**.

Step 12 Click **Submit**.

Step 13 Assign **allPorts** to role MM-role-prod under the **Assign** tab.
The role MM-role-dev now has App-Administrator permissions to the network **dev** and the role MM-role-prod has App-User permissions to network **prod**. You can now create a user that has both of these application roles. Refer to the *Cisco Extensible Network Controller Configuration Guide, Release 1.6* for the procedure to create users.

Note Press Ctrl+F5, or Cmd+Shift+R, simultaneously, when switching between networks with different access levels.

Removing a Role

Note You cannot remove roles that were created by Cisco Extensible Network Controller (XNC).

Step 1 From 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 From 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 can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").

Step 4 Click **Submit**.

What to Do Next

Add resources to the group.

Adding Resources to a Resource Group

Before You Begin

Create a resource group.

Step 1 From 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 Remove a resource, or multiple resources, by choosing one or more ports in the **Group Detail** table, and then clicking **Remove Ports**.

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

What to Do Next

Assign the resource group to a role.

Assigning a Group to a Role

Before You Begin

- Create a role.
- Create a resource group.

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

Step 2 Click 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	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	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 From the **Admin** drop-down list, choose **Settings**.

Step 2 Click 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**.

Removing a Group

The following groups cannot be removed:

- The default **allPorts** group
- Any group that has been assigned to a role.

Step 1 From 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**.