END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT (“AGREEMENT”) BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. The Parties. The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer’s principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer’s principal office is located outside the Americas) (such applicable entity being referred to herein as “Juniper”), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software (“Customer”) (collectively, the “Parties”).

2. The Software. In this Agreement, “Software” means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. “Software” also includes updates, upgrades and new releases of such software. “Embedded Software” means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. License Grant. Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees, provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer’s use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer’s use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

d. For any trial copy of the Software, Customer’s right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer’s enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. Use Prohibitions. Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any ‘locked’ or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. Audit. Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.
6. Confidentiality. The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer’s internal business purposes.

7. Ownership. Juniper and Juniper’s licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. Warranty, Limitation of Liability, Disclaimer of Warranty. The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the “Warranty Statement”). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper’s or its suppliers’ or licensors’ liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. Termination. Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer’s possession or control.

10. Taxes. All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer’s payment of any withholding taxes, completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer’s non-compliance or delay with its responsibilities herein. Customer’s obligations under this Section shall survive termination or expiration of this Agreement.

11. Export. Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer’s ability to export the Software without an export license.

12. Commercial Computer Software. The Software is “commercial computer software” and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT IV) as applicable.

13. Interface Information. To the extent required by applicable law, and at Customer’s written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. Third Party Software. Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License (“GPL”) or the GNU Library General Public License (“LGPL”)), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at http://www.gnu.org/licenses/gpl.html, and a copy of the LGPL at http://www.gnu.org/licenses/lgpl.html.

15. Miscellaneous. This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous
agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présents confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language).)
# Table of Contents

## About This Guide

- Objectives ................................................................. xvi
- Audience ................................................................. xvi
- Documentation Conventions ........................................... xv
- Documentation .......................................................... xvii
- Requesting Technical Support ......................................... xviii
  - Self-Help Online Tools and Resources ......................... xix
  - Opening a Case with JTAC ......................................... xix

## Part 1

### Getting Started

#### Chapter 1

- Getting Started with NSM .............................................. 3
  - Introduction to Network and Security Manager ............... 3
  - Installing NSM .......................................................... 3
  - Role-Based Administration ......................................... 4

#### Chapter 2

- Understanding the JUNOS CLI and NSM ......................... 5
  - NSM and Device Management Overview ....................... 5
  - Understanding the CLI and NSM ................................. 6
  - Comparing the CLI To the NSM UI ............................. 6
  - NSM Services Supported for M-series and MX-series Devices .................. 9
  - How NSM Works with the CLI and Distributed Data Collection .......... 10
  - Device Schemas .......................................................... 12
  - Communication Between a Device and NSM .................... 12
Chapter 11  Viewing the M-series and MX-series Device Inventory in NSM and the CLI  83

Viewing and Reconciling Device Inventory ....................................................83
Comparing Device Inventory in NSM and the CLI ..........................................84
  Viewing Device Inventory in NSM ..........................................................84
  Viewing Device Inventory from the CLI ..................................................86

Chapter 12  Topology Manager  89

Overview of the NSM Topology Manager .....................................................89
Requisites for a Topology Discovery ...........................................................89
About the NSM Topology Manager Toolbar .................................................90

Part 5  Monitoring M-series and MX-series Devices

Chapter 13  Real Time Monitoring of M-series and MX-series  95

About the Realtime Monitor ........................................................................95
Viewing Device Status ..............................................................................96
Viewing Device Monitor Alarm Status ......................................................99
Setting the Polling Interval For Device Alarm Status ...............................100

Part 6  Index

Index .........................................................................................................103
# List of Figures

## Part 1  Getting Started

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Understanding the JUNOS CLI and NSM</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Figure 1: Overview of the User Interface</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Figure 2: NSM Network Architecture</td>
<td>11</td>
</tr>
</tbody>
</table>

## Part 2  Integrating M-series and MX-series Devices

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Updating M-series and MX-series Devices Overview</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Figure 3: Job Information Dialog Box</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Figure 4: Failed Update Job Information Dialog Box</td>
<td>36</td>
</tr>
</tbody>
</table>

## Part 3  Configuring M-series and MX-series Devices

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Configuring M-series and MX-series Devices Overview</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>Figure 5: MPLS Configuration in the CLI</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Figure 6: MPLS Configuration in NSM</td>
<td>46</td>
</tr>
</tbody>
</table>

## Part 4  Managing M-series and MX-series Devices

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Viewing the M-series and MX-series Device Inventory in NSM and the CLI</td>
<td>83</td>
</tr>
<tr>
<td></td>
<td>Figure 7: The Device Inventory Window</td>
<td>85</td>
</tr>
<tr>
<td></td>
<td>Figure 8: Viewing the Hardware Inventory</td>
<td>85</td>
</tr>
<tr>
<td></td>
<td>Figure 9: Viewing the Software Inventory</td>
<td>86</td>
</tr>
</tbody>
</table>
# List of Tables

About This Guide

- Table 1: Notice Icons ................................................................. xvi
- Table 2: Text Conventions .......................................................... xvi
- Table 3: Syntax Conventions ........................................................ xvii
- Table 4: Network and Security Manager Publications .................. xvii

## Part 1

### Getting Started

- Chapter 3: Before You Begin Adding M-series and MX-series Devices 15
  - Table 5: M-series Internet Routers and MX-series Internet Service Routers .............................................................. 15

## Part 2

### Integrating M-series and MX-series Devices

- Chapter 5: Updating M-series and MX-series Devices Overview 29
  - Table 6: Device States During Update ..................................... 34

## Part 3

### Configuring M-series and MX-series Devices

- Chapter 6: Configuring M-series and MX-series Devices Overview 41
  - Table 7: The JUNOS Configuration Hierarchy and the NSM Configuration Tree ........................................................................ 42
- Chapter 7: Configuring Authentication 47
  - Table 8: RADIUS Authentication Configuration Details ............ 47
  - Table 9: TACACS+ Authentication Configuration Details .......... 48
  - Table 10: Login Class Authentication Configuration Details ....... 50
  - Table 11: User Authentication Configuration Details ................. 51
  - Table 12: Remote Template Account Details ............................. 52
  - Table 13: Local Template Account Details ............................... 53
- Chapter 8: Configuring Class of Service Features 55
  - Table 14: Configuring and Applying Behavior Aggregate Classifiers .... 56
  - Table 15: Configuring Code Point Aliases ................................. 58
  - Table 16: Drop Profile Configuration Fields .............................. 59
  - Table 17: Assigning Forwarding Classes to Output Queues .......... 61
  - Table 18: Interfaces Configuration Fields ................................. 63
  - Table 19: Configuring and Applying Rewrite Rules ..................... 68
  - Table 20: Configuring Schedulers ............................................. 71
  - Table 21: Assigning Forwarding Classes to Output Queues .......... 73
- Chapter 9: Configuring SNMP 75
  - Table 22: Basic System Identification Details ............................. 75
Table 23: SNMP Agents and Community Configuration Details .....................76
Table 24: SNMP Trap Group Configuration Details ........................................77
Table 25: SNMP View Configuration Details ..................................................78

Part 5

Monitoring M-series and MX-series Devices

Chapter 13
Real Time Monitoring of M-series and MX-series ....................................95
Table 26: Device Status Information ..............................................................96
About This Guide

Objectives

- Objectives on page xv
- Audience on page xv
- Documentation Conventions on page xv
- Documentation on page xvii
- Requesting Technical Support on page xviii

Objectives

Juniper Networks Network and Security Manager (NSM) is a software application that centralizes control and management of your Juniper Networks devices. With NSM, Juniper Networks delivers integrated, policy-based security and network management for all devices.

M-series and MX-series devices are routers that run JUNOS software using the command-line interface (CLI) for installation and configuration.

This guide provides the information you need to understand, configure, and maintain an M-series or MX-series device using NSM. This guide explains how to use basic NSM functionality, including adding new devices, deploying new device configurations, updating device firmware, and monitoring the status of your M-series or MX-series device. Use this guide in conjunction with the NSM Online Help, which provides step-by-step instructions that complement the information in this guide.

NOTE: If the information in the latest NSM Release Notes differs from the information in this guide, follow the NSM Release Notes.

Audience

This guide is for the system administrator responsible for configuring the M-series and MX-series devices.

Documentation Conventions

The sample screens used throughout this guide are representations of the screens that appear when you install and configure the NSM software. The actual screens may differ.
All examples show default file paths. If you do not accept the installation defaults, your paths will vary from the examples.

Table 1 on page xvi defines notice icons used in this guide.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📝</td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td>⚠️🌟</td>
<td>Laser warning</td>
<td>Alerts you to the risk of personal injury from a laser.</td>
</tr>
</tbody>
</table>

Table 2 on page xvi defines text conventions used in this guide.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bold typeface like this</td>
<td>Represents commands and keywords in text. Represents keywords Represents UI elements</td>
<td>Issue the <strong>clock source</strong> command. Specify the keyword <strong>exp-msg</strong> Click <strong>User Objects</strong></td>
</tr>
<tr>
<td>Bold typeface like this</td>
<td>Represents text that the user must type.</td>
<td>user input</td>
</tr>
<tr>
<td>fixed-width font</td>
<td>Represents information as displayed on the terminal screen.</td>
<td><code>host1# show ip ospf</code> Routing Process OSPF 2 with Router ID 5.5.0.250 Router is an area Border Router (ABR)</td>
</tr>
<tr>
<td>Key names linked with a plus (+) sign</td>
<td>Indicates that you must press two or more keys simultaneously.</td>
<td>Ctrl + d</td>
</tr>
<tr>
<td><em>Italics</em></td>
<td>Emphasizes words Identifies variables</td>
<td>The product supports two levels of access, user and privileged. <code>clusterID</code>, <code>ipAddress</code></td>
</tr>
<tr>
<td>The angle bracket (&gt;)</td>
<td>Indicates navigation paths through the UI by clicking menu options and links.</td>
<td>Object Manager &gt; User Objects &gt; Local Objects</td>
</tr>
</tbody>
</table>
Table 3 on page xvii defines syntax conventions used in this guide.

### Table 3: Syntax Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Words in plain text</td>
<td>Represent keywords</td>
<td>terminal length</td>
</tr>
<tr>
<td>Words in italics</td>
<td>Represent variables</td>
<td>mask, accessListName</td>
</tr>
<tr>
<td>Words separated by the pipe `</td>
<td>` symbol</td>
<td>Represent a choice to select one keyword or variable to the left or right of this symbol. The keyword or variable can be optional or required.</td>
</tr>
<tr>
<td>Words enclosed in brackets <code>[ ]</code></td>
<td>Represent optional keywords or variables.</td>
<td>[ internal</td>
</tr>
<tr>
<td>Words enclosed in brackets followed by and asterisk <code>[ ]*</code></td>
<td>Represent optional keywords or variables that can be entered more than once.</td>
<td>[ level1</td>
</tr>
<tr>
<td>Words enclosed in braces <code>{ }</code></td>
<td>Represent required keywords or variables.</td>
<td>{ permit</td>
</tr>
</tbody>
</table>

### Documentation

Table 4 on page xvii describes documentation for the NSM.

### Table 4: Network and Security Manager Publications

<table>
<thead>
<tr>
<th>Book</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network and Security Manager Installation Guide</td>
<td>Describes the steps to install the NSM management system on a single server or on separate servers. It also includes information on how to install and run the NSM user interface. This guide is intended for IT administrators responsible for the installation or upgrade of NSM.</td>
</tr>
<tr>
<td>Network and Security Manager Administration Guide</td>
<td>Describes how to use and configure key management features in the NSM. It provides conceptual information, suggested workflows, and examples. This guide is best used in conjunction with the NSM Online Help, which provides step-by-step instructions for performing management tasks in the NSM UI. This guide is intended for application administrators or those individuals responsible for owning the server and security infrastructure and configuring the product for multi-user systems. It is also intended for device configuration administrators, firewall and VPN administrators, and network security operation center administrators.</td>
</tr>
<tr>
<td>Network and Security Manager Configuring ScreenOS and IDP Devices Guide</td>
<td>Provides details about configuring the device features for all supported ScreenOS and IDP platforms.</td>
</tr>
<tr>
<td>Book</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network and Security Manager Online Help</td>
<td>Provides procedures for basic tasks in the NSM user interface. It also includes a brief overview of the NSM system and a description of the GUI elements.</td>
</tr>
<tr>
<td>Network and Security Manager API Guide</td>
<td>Provides complete syntax and description of the SOAP messaging interface to NSM.</td>
</tr>
<tr>
<td>Network and Security Manager Release Notes</td>
<td>Provides the latest information about features, changes, known problems, resolved problems, and system maximum values. If the information in the Release Notes differs from the information found in the documentation set, follow the Release Notes. Release notes are included on the corresponding software CD and are available on the Juniper Networks Website.</td>
</tr>
<tr>
<td>Configuring Infranet Controllers Guide</td>
<td>Provides details about configuring the device features for all supported Infranet Controllers.</td>
</tr>
<tr>
<td>Configuring Secure Access Devices Guide</td>
<td>Provides details about configuring the device features for all supported Secure Access Devices.</td>
</tr>
<tr>
<td>Configuring EX-series Switches Guide</td>
<td>Provides details about configuring the device features for all supported EX-series platforms.</td>
</tr>
<tr>
<td>M-series and MX-series Devices Guide</td>
<td>Provides details about configuring the device features for M-series and MX-series platforms.</td>
</tr>
</tbody>
</table>

**Requesting Technical Support**

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- ** Product warranties—**For product warranty information, visit [http://www.juniper.net/support/warranty/](http://www.juniper.net/support/warranty/).
- ** JTAC Hours of Operation —**The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.
Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool located at https://tools.juniper.net/SerialNumberEntitlementSearch/.

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting support.html
M-series and MX-series Devices

XX  Requesting Technical Support
Part 1
Getting Started

- Getting Started with NSM on page 3
- Understanding the JUNOS CLI and NSM on page 5
- Before You Begin Adding M-series and MX-series Devices on page 15
M-series and MX-series Devices
Chapter 1
Getting Started with NSM

Introduction to Network and Security Manager

Juniper Networks Network and Security Manager (NSM) gives you complete control over your network. Using NSM, you can configure all your Juniper Networks devices from one location, at one time.

NSM works with networks of all sizes and complexity. You can add a single device, or create device templates to help you deploy multiple devices. You can create new policies, or edit existing policies for security devices. The management system tracks and logs each administrative change in real time, providing you with a complete administrative record and helping you perform fault management.

NSM also simplifies control of your network with a straightforward user interface. Making all changes to your devices from a single, easy-to-use interface can reduce deployment costs, simplify network complexity, speed configuration, and minimize troubleshooting time.

For more detailed information about NSM, including a technical overview, working in the NSM user interface (UI), and new features in NSM 2008.2, see the section on getting started with NSM in the *Network and Security Manager Administration Guide*.

Related Topics

- Installing NSM on page 3
- Role-Based Administration on page 4
- NSM and Device Management Overview on page 5

Installing NSM

NSM is a software application that enables you to integrate and centralize management of your Juniper Networks environment. You need to install two main software components to run NSM: the NSM management system and the NSM user interface (UI).
The overall process for installing NSM is as follows:

- Management System Installation Process
- User Interface Installation Process

Refer to the *Network Security Manager Installation Guide* for details on the steps to install the NSM management system on a single server or on separate servers. It also includes information on how to install and run the NSM user interface. The *Network Security Manager Installation Guide* is intended for IT administrators responsible for the installation of or upgrade to NSM.

**Role-Based Administration**

The NSM role-based administration (RBA) feature enables you to define strategic roles for your administrators, delegate management tasks, and enhance existing permission structures using task-based functions.

Use NSM to create a secure environment that reflects your current administrator roles and responsibilities. By specifying the exact tasks your NSM administrators can perform within a domain, you minimize the probability of errors and security violations and enable a clear audit trail for every management event.

For more detailed information about role-based administration, including using role-based administration more effectively and configuring role-based administration, see “Configuring Role-Based Administration” in the *Network and Security Manager Administration Guide*.

**Related Topics**

- Introduction to Network and Security Manager on page 3
- Role-Based Administration on page 4
- NSM and Device Management Overview on page 5
Chapter 2
Understanding the JUNOS CLI and NSM

- NSM and Device Management Overview on page 5
- Understanding the CLI and NSM on page 6
- Comparing the CLI To the NSM UI on page 6
- NSM Services Supported for M-series and MX-series Devices on page 9
- How NSM Works with the CLI and Distributed Data Collection on page 10
- Device Schemas on page 12
- Communication Between a Device and NSM on page 12

NSM and Device Management Overview

NSM is the Juniper Networks network management tool that allows distributed administration of network appliances like the M-series and MX-series routers. You can use the NSM application to centralize status monitoring, logging, and reporting, and to administer device configurations. The term device is used in NSM to describe a router or platform.

With NSM you can manage and administer a device from a single management interface.

In addition, NSM lets you manage most of the parameters that you can configure through the command-line interface (CLI). Although the configuration screens rendered in NSM look different, the top-level configuration elements essentially correspond to commands in the CLI.

NSM incorporates a broad configuration management framework that allows co-management using other methods. To manage the device configuration, you can also use the XML files import and export feature, or you can manage from the device’s admin console.

Related Topics
- Understanding the CLI and NSM on page 6
- Comparing the CLI To the NSM UI on page 6
- NSM Services Supported for M-series and MX-series Devices on page 9
- How NSM Works with the CLI and Distributed Data Collection on page 10
- Device Schemas on page 12
- Communication Between a Device and NSM on page 12
Understanding the CLI and NSM

M-series and MX-series devices are routers that have the JUNOS software installed as the operating system. With the JUNOS software you use the command-line interface (CLI) to access an individual router (which is called a device in NSM)—whether from the console or through a network connection. The CLI is a JUNOS software-specific command shell that runs on top of a UNIX-based operating system kernel. The CLI is a straightforward command interface you can use to monitor and configure a router. You type commands on a single line, and the commands are executed when you press the Enter key. For more information on the CLI, see the JUNOS CLI User Guide.

Network and Security Manager (NSM) is a software application that centralizes control and management of your Juniper Networks devices. NSM is a three-tier management system made up of the following:

- A user interface (UI)
- Management system
- Managed devices

The devices process your network traffic and are the enforcement points that implement your policies. The UI and management system tiers are software-based so you can deploy them quickly and easily. Because the management system uses internal databases for storage and authentication, you do not need LDAP or an external database. For more information about NSM architecture, see the technical overview in the Network Security Manager Administration Guide.

With NSM you can manage most of the parameters that you can configure through the CLI. Although the configuration screens rendered in NSM look different, the top-level configuration elements essentially correspond to commands in the CLI.

Typically, M-series and MX-series devices are managed individually using the CLI. The advantage of using NSM is that you can centralize status monitoring and administration of the configurations of a network of M-series and MX-series devices.

Related Topics
- NSM and Device Management Overview on page 5
- Comparing the CLI To the NSM UI on page 6
- NSM Services Supported for M-series and MX-series Devices on page 9
- How NSM Works with the CLI and Distributed Data Collection on page 10
- Device Schemas on page 12
- Communication Between a Device and NSM on page 12

Comparing the CLI To the NSM UI

Because NSM is a UI and the CLI is a command-line interface, the way you access configuration, monitoring, and management information is different in each interface. The CLI has two modes: operational mode and configuration mode.
Operational mode—This mode displays the current router status. In operational mode, you enter commands to monitor and troubleshoot the software, network connectivity, and router.

Configuration mode—A router configuration is stored as a hierarchy of statements. In configuration mode, you enter these statements to define all properties of the JUNOS software, including interfaces, general routing information, routing protocols, user access, and several system hardware properties.

The following sample output shows the operational mode commands available at the top level of the CLI operational mode:

```
user@host> ?
Possible completions:
  clear                Clear information in the system
  configure            Manipulate software configuration information
  file                 Perform file operations
  help                 Provide help information
  monitor              Show real-time debugging information
  mtrace               Trace multicast path from source to receiver
  op                   Invoke an operation script
  ping                 Ping remote target
  quit                 Exit the management session
  request              Make system-level requests
  restart              Restart software process
  set                  Set CLI properties, date/time, craft interface message
  show                 Show system information
  ssh                  Start secure shell on another host
  start                Start shell
  telnet               Telnet to another host
  test                 Perform diagnostic debugging
  traceroute           Trace route to remote host
```

The following sample output shows the protocols configuration of an M-series device:

```
[edit]
user@host# show protocols
mpls {
  interface ge-1/3/3.0;
  interface fe-0/1/2.0;
  interface fe-0/1/1.0;
}
ospf {
  traffic-engineering;
  area 0.0.0.1 {
    interface lo0.0 {
      passive;
    }
    interface ge-1/3/3.0;
    interface fe-0/1/2.0;
    interface fe-0/1/1.0;
  }
}
```

For more information about operational and configuration mode, see the JUNOS CLI User Guide.
In contrast, the NSM UI displays a set of menus, toolbar icons at the top of the UI window, and a navigation tree that includes an Investigate panel, a Configure panel, and an Administer panel. For some components, right-click menus are available to perform tasks.

Figure 1 on page 8 shows the NSM UI with the Configure navigation tree expanded and the main display area containing the services available from the Configure panel. Different services display when you select the Investigate or Administer panels.

**Figure 1: Overview of the User Interface**

- **Menu bar**—Contains clickable commands. You can access many menu bar commands using keyboard shortcuts. For a complete list of keyboards shortcuts, see the *Network and Security Manager Online Help*.
- **Toolbar**—Contains buttons for common tasks. The buttons displayed in the toolbar are determined by the selected module.
Domain menu—Contains a pull-down menu above the navigation tree where domains and subdomains are selected. The domains and subdomains displayed are those to which the current user has access.

Navigation Tree—The navigation tree displays the 11 NSM modules in the left pane of the NSM window.

Investigate panel—Provides NSM modules with tree structures for monitoring your network.

Configure panel—Provides NSM modules with tree structures for configuring devices, policies, virtual private networks (VPNs), and other objects.

Administer panel—Provides NSM modules with tree structures for managing the NSM servers, ongoing jobs, and other actions.

Main display area—Displays the content for the currently selected module or module contents.

Common tasks pane—Provides links to commonly accessed tasks throughout the UI. These common tasks change depending on what tasks are often selected in the UI.

Status bar—Displays additional information for a selected module.

For details about the Investigate, Configure, and Administer panels, see “NSM Modules” in the Network Security Manager Administration Guide.

NSM Services Supported for M-series and MX-series Devices

NSM supports the following services for the M-series and MX-series devices:

- Device management—Enables addition of new devices, editing and deletion of existing devices, software version update, reconfiguration of existing devices, activation of modeled devices, and master Routing Engine switchover with synchronized commits. In addition, Return Merchandise Authorization (RMA) updates enable failed device replacement without a serial number or connection statistics.

- Device discovery—Uses sets of rules to find, add, and import multiple devices into NSM. In addition, configure and run rules to search a network and find devices in a specified subnet, or within a specified range of IP addresses. M-series and MX-series devices must be configured with static IP addresses to be found by device discovery rules.

- Topology management—Provides discovery and management of the physical topology of a network of devices connected to a Juniper Networks EX-series
switch. These include networking devices such as the J-series, M-series, MX-series and EX-series as well as ScreenOS and Intrusion Detection and Prevention (IDP) devices, IP phones, desktops, printers, and servers. The Topology Manager also provides details about connections between a device and the EX-series switch.

- Inventory and license management—Displays device inventory and licensing details. In a dual Routing Engine system, the inventory data is collected from the master Routing Engine.
- Upgrading software for single and dual Routing Engines.
- Configuration management—Enables in-device configuration and editing, configuration groups, and template configuration.
- Status monitoring—Displays a list of all managed devices, including status, name, domain, OS version, synchronization status, connection details, and current alarms.
- Job management—Displays details of the update process in a dedicated information window and includes the update’s success or failure and the errors involved in a failed update.

Below is a summary of the services that are not supported for the M-series and MX-series devices:

- Adding, deleting, or editing licensing information, (though licenses can be viewed).
- Downgrading software.
- Configuration of cluster objects, policy manager, VPN manager, and shared objects.
- JUNOS Redundancy Protocol (JSRP), VPN, and IDP cluster monitor.

### Related Topics

- NSM and Device Management Overview on page 5
- Understanding the CLI and NSM on page 6
- Comparing the CLI To the NSM UI on page 6
- How NSM Works with the CLI and Distributed Data Collection on page 10
- Device Schemas on page 12
- Communication Between a Device and NSM on page 12

### How NSM Works with the CLI and Distributed Data Collection

Before we can discuss how NSM works with the CLI, the following terms need to be defined:

- ADM (Abstract Data Model)—The Abstract Data Model is an XML file that contains all the configuration information for a domain.
- configlet—A configlet is a small, static configuration file that contains information on how a device can connect to NSM.
- Device Server—The Device Server is the component of the NSM management system that handles communication between the GUI Server and the device,
collects data from the managed devices on your network, formats configuration information sent to your managed device, and consolidates log and event data.

- **DM (Data Model)**—A Data Model is an XML file that contains configuration data for an individual device. The DM is stored in the Device Server; when you create, update, or import a device, the GUI Server edits the Abstract Data Model (ADM) to reflect the changes, then translates that information to the DM.

- **GUI Server**—The GUI Server manages the system resources and data that drives NSM functionality. The GUI Server contains the NSM databases and centralizes information for devices and their configurations, attack and server objects, and policies.

NSM and the CLI communicate through the GUI and Device Servers that translate objects and object attributes in both directions. Device configuration information is translated into Data Model (DM) objects or Abstract Data Model (ADM) object attributes, and conversely DM objects and ADM object attributes are translated into XML configlets and documents.

NSM uses a distributed data collection system. Each device is described by a unique DM. The DM is stored in the Device Server which communicates with the GUI Server and the device.

When you create, update, or import a device into NSM, the GUI Server edits the ADM to reflect the changes, then translates that information to the DM. The ADM contains configuration data for all objects in a specific domain. When you use the UI to interface with your managed devices, the ADM and DMs work together.

**Figure 2: NSM Network Architecture**

- When you update a device configuration, the GUI Server translates the objects and object attributes in the ADM domain into device configuration information in a DM. For DMI based devices which include the M-series and MX-series, the Device Server converts the DM into an XML configlet and sends the configlet through NetConf protocol to the device.

- When you import a device configuration, the device sends the configuration through the NetConf protocol as an XML document to the Device Server, which translates the XML document into a DM with device configuration information.
The GUI Server then translates the device configuration in the DM into objects and object attributes in the ADM, and uses the ADM to display current information in the UI.

For more details on the ADM and DMs, see “Managing Devices” in the Network Security Manager Administration Guide.

The management system also provides an application programming interface (API) for integrating NSM into larger enterprise business systems. This NSM API provides an alternative interface to that provided by the UI. For details, see the Network and Security Manager API Guide.

Related Topics
■ NSM and Device Management Overview on page 5
■ Understanding the CLI and NSM on page 6
■ Comparing the CLI To the NSM UI on page 6
■ NSM Services Supported for M-series and MX-series Devices on page 9
■ Device Schemas on page 12
■ Communication Between a Device and NSM on page 12

Device Schemas

The structure of the ADM and the DMs is defined by a DM schema, which lists all the possible fields and attributes for a type of object or device. The DM schema reads from a capability file, which lists the fields and attributes that a specific operating system version supports, to determine the supported features for the operating system version that is running on the managed devices. NSM uses capability files to enable JUNOS software upgrades without changing the device configuration in NSM.

The M-series and MX-series device families are described by schemas that are maintained on a schema repository owned by Juniper Networks. These schemas can be added dynamically to NSM.

Related Topics
■ NSM and Device Management Overview on page 5
■ Understanding the CLI and NSM on page 6
■ Comparing the CLI To the NSM UI on page 6
■ NSM Services Supported for M-series and MX-series Devices on page 9
■ How NSM Works with the CLI and Distributed Data Collection on page 10
■ Communication Between a Device and NSM on page 12

Communication Between a Device and NSM

The M-series and MX-series devices and the NSM application communicate through the Device Management Interface (DMI). DMI is a collection of schema-driven protocols that run on a common transport (TCP). DMI is designed to work with routers running the JUNOS software to make device management consistent across all
administrative realms. The DMI protocols that are supported include NetConf (for inventory management, XML-based configuration, text-based configuration, alarm monitoring, and device-specific commands), structured syslog, and threat flow for network profiling. DMI supports third-party network management systems that incorporate the DMI standard; however, only one DMI-based agent per device is supported.

The configuration of the M-series and MX-series device is represented as a hierarchical tree of configuration items. This structure is expressed in XML that can be manipulated with NetConf. NetConf is a network management protocol that uses XML. DMI uses NetConf’s generic configuration management capability and applies it to allow remote configuration of the device.

The schema repository enables access to XSD and XML files defined for each device, model, and software version.

**Related Topics**
- NSM and Device Management Overview on page 5
- Understanding the CLI and NSM on page 6
- Comparing the CLI To the NSM UI on page 6
- NSM Services Supported for M-series and MX-series Devices on page 9
- How NSM Works with the CLI and Distributed Data Collection on page 10
- Device Schemas on page 12
Chapter 3
Before You Begin Adding M-series and MX-series Devices

- M-series and MX-series Devices Supported by NSM on page 15
- Considering the Device Status on page 16
- Configuring a Deployed M-series or MX-series Device for Importing to NSM on page 17

M-series and MX-series Devices Supported by NSM

Table 5 on page 15 lists the M-series Internet routers, MX-series Internet Services routers, and the operating system versions supported by NSM.

Table 5: M-series Internet Routers and MX-series Internet Service Routers

<table>
<thead>
<tr>
<th>Device</th>
<th>Operating System Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Juniper Networks M7i Internet router</td>
<td>JUNOS Release 9.3</td>
</tr>
<tr>
<td>Juniper Networks M10i Internet router</td>
<td>JUNOS Release 9.3</td>
</tr>
<tr>
<td>Juniper Networks M40e Internet router</td>
<td>JUNOS Release 9.3</td>
</tr>
<tr>
<td>Juniper Networks M120 Internet router</td>
<td>JUNOS Release 9.3</td>
</tr>
<tr>
<td>Juniper Networks M320 Internet router</td>
<td>JUNOS Release 9.3</td>
</tr>
<tr>
<td>Juniper Networks MX240 Internet Services router</td>
<td>JUNOS Release 9.3</td>
</tr>
<tr>
<td>Juniper Networks MX480 Internet Services router</td>
<td>JUNOS Release 9.3</td>
</tr>
<tr>
<td>Juniper Networks MX960 Internet Services router</td>
<td>JUNOS Release 9.3</td>
</tr>
</tbody>
</table>

Related Topics
- Considering the Device Status on page 16
- Configuring a Deployed M-series or MX-series Device for Importing to NSM on page 17
**Considering the Device Status**

The network status of your device influences the preliminary configuration required before you can add the device to NSM and the method you use to add the device to NSM. Devices can be deployed in your network or undeployed. Deployed devices can be configured with a static or dynamic IP address, which influences the method you use to add them to NSM. Also, undeployed devices are treated differently from deployed devices.

- **Deployed devices**—Deployed devices are the devices you are currently using in your existing network. These devices have already been configured with a static or dynamic IP address and other basic information. You can import a device with a static or dynamic IP address to NSM, so long as it has the following enabled:
  - The management interface (fxp0) with the IP address of the device and a user with full administrative privileges for the NSM administrator.
  - A physical connection to your network with access to network resources.
  - Connectivity to the NSM device server, which can be with a static IP address.
  - Telnet or SSHv2, and NETCONF protocol over SSH.

The NSM process of importing a deployed device differs depending on whether your device is configured with a static or dynamic IP address. For information about importing a device with a static IP address or about importing a device with a dynamic IP address, see the *Network Security Manager Administration Guide*.

**NOTE:** To import device configurations, the connection between NSM and the managed device must be at least 28.8 Kbps. For details on installing NSM on your network, refer to the *Network and Security Manager Installation Guide*.

- **Undeployed devices**—Undeployed devices are devices that you are not currently using in your network and, typically, for which you do not have IP addresses, zones, or other basic network information. For undeployed devices, you can model a new device configuration and later install that configuration on the device. For more information on adding undeployed devices, see “Modeling a Device” in the *Network Security Manager Administration Guide*.

**Related Topics**
- M-series and MX-series Devices Supported by NSM on page 15
- Configuring a Deployed M-series or MX-series Device for Importing to NSM on page 17
**Configuring a Deployed M-series or MX-series Device for Importing to NSM**

A deployed device is a device you are currently using in your network. Before you can add a deployed device to NSM, you must configure the following parameters on the device, regardless of the static or dynamic nature of the IP address:

- The management interface (fxp0) with the IP address of the device
- A user with full administrative privileges for the NSM administrator
- A physical connection to your network with access to network resources
- Connectivity to the NSM device server, which can be with a static IP address
- Telnet or SSHv2, and NETCONF protocol over SSH

To configure these parameters, perform the following tasks:

- Configure an IP Address and a User with Full Administrative Privileges for the Device on page 17
- Check Network Connectivity on page 17
- Check Connectivity to the NSM Server on page 18
- Configure a Static Route to the NSM Server on page 18
- Establish a Telnet or an SSHv2, and a NETCONF protocol over SSH Connection to the NSM Server on page 19

**Configure an IP Address and a User with Full Administrative Privileges for the Device**

**Purpose**  
Before you can add an M-series or MX-series device to NSM, you must have an IP address configured on the management interface (fxp0) and a user with full administrative privileges for the NSM administrator.

**Action**  
Generally when you install the JUNOS software, you configure the router from scratch and at that point you configure the management interface (fxp0) with the IP address and a user with full administrative privileges.

For information on configuring the router from scratch, see the *JUNOS System Basics Configuration Guide*.

For step-by-step instructions on reconfiguring names, addresses, and the root password after reinstalling the JUNOS software, see “Configure Names and Addresses” and “Set the Root Password.”

**Check Network Connectivity**

**Purpose**  
Establish that the M-series or MX-series device has a connection to your network.

**Action**  
To check that the device has a connection to your network, log on to the M-series or MX-series device and issue a `ping` command to a system on your network:

```
root@> ping address
```
If there is no response, verify that there is a route to the `address` using the `show route` command. If the address is outside your `fxp0` subnet, add a static route.

**Check Connectivity to the NSM Server**

**Purpose** Establish that the M-series or MX-series device has a connection to the NSM server.

**Action** To check that the device has a connection to the NSM server, log on to the M-series or MX-series device and issue a `ping` command to the IP address of the NSM server:

```
root@>
```

ping address

If there is no response, verify that there is a route to the `address` using the `show route` command. If the address is outside your `fxp0` subnet, add a static route.

**Configure a Static Route to the NSM Server**

**Purpose** When your M-series or MX-series device and the NSM server are in different subnets, you can install a static route on the device to connect to the NSM server. The static route is installed in the routing table only when the route is active; that is, the list of next-hop routers configured for that route contains at least one next hop on an operational interface.

**Action** To configure a static route, follow these steps:

1. Log on to the M-series or MX-series device and, in configuration mode, go to the following hierarchy level:

   `[edit]`

   user@host# edit routing-options

2. Configure a static route to the NSM server with the `retain` option so that the static route remains in the forwarding table when the routing protocol process shuts down normally:

   `[edit routing-options]`

   user@host# set static route destination-prefix next-hop address retain

3. Configure the `no-readvertise` option so that the route is not eligible for readvertisement by dynamic routing protocols:

   `[edit routing-options]`

   user@host# set static route destination-prefix next-hop address no-readvertise

4. Verify the configuration:

   user@host# show

5. Commit the configuration:

   user@host# commit

6. Verify the connection to the NSM server:
user@host# run ping destination

Sample Output

user@host> edit
Entering configuration mode
[edit]
user@host# edit routing-options
[edit routing-options]
user@host# set static route 192.193.60.181/32 next-hop 192.193.76.254
[edit routing-options]
user@host# set static route 192.193.60.181/32 retain
[edit routing-options]
user@host# set static route 192.193.60.181/32 no-readvertise
[edit routing-options]
user@host# show
static {
    route 192.193.60.181/32 {
        next-hop 192.193.76.254;
        retain;
        no-readvertise;
    }
}
[edit routing-options]
user@host# commit
commit complete
[edit routing-options]
user@host# run ping 192.193.60.181
PING 192.193.60.181 (192.193.60.181): 56 data bytes
64 bytes from 192.193.60.181: icmp_seq=0 ttl=64 time=23.050 ms
64 bytes from 192.193.60.181: icmp_seq=1 ttl=64 time=18.129 ms
64 bytes from 192.193.60.181: icmp_seq=2 ttl=64 time=0.304 ms
^C
--- 192.193.60.181 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.304/13.828/23.050/9.771 ms

Meaning
The sample output shows that a static route (192.193.60.181/32) to the NSM server is configured and committed, and that there is a connection between the router and the server because the ping command shows that three packets were transmitted and received.

Establish a Telnet or an SSHv2, and a NETCONF protocol over SSH Connection to the NSM Server

To configure an M-series or MX-series device before adding it to NSM, take the following steps:

1. Log on to the M-series or MX-series device.
2. In configuration mode, go to the following hierarchy level:
3. At the [edit system services] hierarchy level, enter the following commands:

```
user@host# set ftp
user@host# set ssh protocol-version v2
user@host# set telnet
user@host# set netconf ssh
```

4. Verify the configuration:

```
user@host# show
```

5. Commit the configuration:

```
user@host# commit
```

**Sample Output**

```
[edit]
user@host# edit system services
[edit system services]
user@host# set ftp
[edit system services]
user@host# set ssh protocol-version v2
[edit system services]
user@host# set telnet
[edit system services]
user@host# set netconf ssh
[edit system services]
user@host# show
ftp;
ssh {
  protocol-version v2;
}
telnet;
etconf {
  ssh;
}
[edit system services]
user@host# commit
commit complete
```
Part 2

Integrating M-series and MX-series Devices

- Adding M-series and MX-series Devices Overview on page 23
- Updating M-series and MX-series Devices Overview on page 29
Chapter 4
Adding M-series and MX-series Devices
Overview

■ About Device Creation on page 23
■ Supported Add Device Workflows for M-series and MX-series Devices on page 24
■ Importing Devices Overview on page 25
■ Modeling Devices Overview on page 26
■ Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only) on page 27
■ Adding Device Groups Overview on page 27

About Device Creation

Before Network and Security Manager (NSM) can manage devices, you must first add those devices to the management system using the NSM user interface (UI). To add a device, you create an object in the UI that represents the physical device, and then create a connection between the UI object and the physical device so that their information is linked. When you make a change to the UI device object, you can push that information to the real device so the two remain synchronized. You can add a single device at a time or add multiple devices all at once.

**NOTE:** The connection between a managed device and the NSM Device Server must be at least 28.8 Kbps.

How you add your devices to the management system depends on the network status of the device. You can import deployed devices, or you can model devices that have not yet been deployed:

■ Import deployed devices—Deployed devices are the devices you are currently using in your existing network. These devices have already been configured with a static or dynamic IP address and other basic information. For deployed devices, you can import the existing device configuration information into NSM.
NOTE: To import device configurations, the connection between NSM and the managed device must be at least 28.8 Kbps. For details on installing NSM on your network, refer to the Network and Security Manager Installation Guide.

- Model undeployed devices—Undeployed devices are devices that you are not currently using in your network and, typically for which, you do not have IP addresses, zones, or other basic network information. For undeployed devices, you can model a new device configuration and later install that configuration on the device.

To help you add a device, the UI contains an Add Device wizard that walks you through each step of the device creation process. The Add Device wizard prompts you to first choose a workflow from the given options. Device is reachable is the default option. The wizard then prompts you for specific device information, such as the device platform name, OS name and version, IP address, and device administrator name, and then uses that information to detect the device. You can then choose to modify the displayed name of the device and assign a color to the device. If the host name is not unique within NSM or is undetected, the Add Device wizard generates a validation error, forcing you to add a valid device name in order to proceed with adding the physical device to the Device Server.

After the physical device connects, it is considered to be a managed device, meaning it is now under the control of NSM.

For more detailed information about verifying and managing a device, see “About Device Creation” in the Network and Security Manager Administration Guide.

Related Topics
- Supported Add Device Workflows for M-series and MX-series Devices
- Importing Devices Overview
- Modeling Devices Overview
- Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only)
- Adding Device Groups Overview

Supported Add Device Workflows for M-series and MX-series Devices

An M-series or MX-series device can be added using the following methods or workflows:

- Import device with static IP address
- Import device with dynamic IP address
- Model and activate device
- Rapid deployment (configlets)
- Device discovery
Import many devices (CSV file) with static IP addresses
Import many devices (CSV file) with dynamic IP addresses

The model many devices (CSV file) workflow is not supported.

Related Topics
- About Device Creation on page 23
- Importing Devices Overview on page 25
- Modeling Devices Overview on page 26
- Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only) on page 27
- Adding Device Groups Overview on page 27

Importing Devices Overview

NSM can import device configurations from M-series and MX-series devices running JUNOS 9.3 or later.

When importing from a device, the management system connects to the device and imports Data Model (DM) information that contains details of the device configuration. The connection is secured using Secure Server Protocol (SSP), a proprietary encryption method; an always-on connection exists between the management system and the device.

For details about adding multiple devices at one time, see the Network and Security Manager Administration Guide.

Requirements
To import a single device, you must have available the following requirements:
- A management interface (fxp0) with the IP address of the device
- A user with full administrative privileges for the NSM administrator
- Device connection information (IP address, connection method) and the device administrator’s name and password

*NOTE:* All passwords handled by NSM are case-sensitive.

- A physical connection to your network with access to network resources
- Connectivity to the NSM Device Server, which can be with a static IP address
- A Telnet or an SSHv2, and a NETCONF protocol over SSH connection
NOTE: After importing a device configuration, log entries from that device begin to appear in the Log Viewer. However, until you update the device from NSM, the following log fields display 0 (or unknown):

- domain
- rulebase
- policy
- rule number
- source zone
- destination zone

After you update the imported device configuration using NSM, the appropriate values are displayed for log entries from the device.

When you import a device configuration, the Log Viewer displays the appropriate values for the device's log entries. This feature eliminates the need to update the device after importing it.

For more detailed information about adding and importing devices with static and dynamic IP addresses and verifying imported device configurations, see “Adding Devices” in the Network and Security Manager Administration Guide.

Related Topics
- About Device Creation on page 23
- Supported Add Device Workflows for M-series and MX-series Devices on page 24
- Modeling Devices Overview on page 26
- Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only) on page 27
- Adding Device Groups Overview on page 27

Modeling Devices Overview

For an undeployed M-series or MX-series device, you can create a device configuration in NSM, and then install that device configuration on the physical device.

Adding a single undeployed device to NSM is a four-stage process:

1. Model the device in the UI.
2. Create the device object configuration.
3. Activate the device.
4. Update the device configuration.
For more detailed information and steps about modeling a device, see “Modeling Devices” in the Network and Security Manager Administration Guide.

**Related Topics**
- About Device Creation on page 23
- Supported Add Device Workflows for M-series and MX-series Devices on page 24
- Importing Devices Overview on page 25
- Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only) on page 27
- Adding Device Groups Overview on page 27

### Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only)

You can use automatic discovery to add and import multiple JUNOS software devices into NSM. You do so by configuring and running discovery rules. For a JUNOS software device to be discovered by this mechanism, it must be configured with a static IP address.

By configuring and running a discovery rule, you can search a network to discover devices in a specified subnet or within a range of IP addresses. Authentication of the devices is through administrator login SSHv2 credentials and SNMP community settings, which you also configure as part of the rule. Devices that match the rules for discovery also present an SSH key for your verification before the device is added to NSM.

For more detailed information and steps about adding multiple M-series and MX-series devices using automatic discovery, see “Adding a Device Discovery Rule” and “Running a Device Discovery Rule” in the Network and Security Manager Administration Guide.

**Related Topics**
- About Device Creation on page 23
- Supported Add Device Workflows for M-series and MX-series Devices on page 24
- Importing Devices Overview on page 25
- Modeling Devices Overview on page 26
- Adding Device Groups Overview on page 27

### Adding Device Groups Overview

You can create groups of devices to manage multiple devices at one time. Use device groups to organize your managed devices, making it easier for you to configure and manage devices within a domain. You can group devices by type (such as all the M-series in a domain), by physical location (such as all the devices in the San Jose office), or logically (such as all the devices in sales offices throughout western Europe).

Use the groups to:
- Deploy new or updated device configurations to the entire device group.
- Deploy new or updated policies to the entire device group.

The devices that you add to a device group must exist; that is, you must have previously added or modeled the devices in the domain. You can group devices before configuring them. You can add a device to more than one device group. You can also add a device group to another device group.

**NOTE:** You cannot apply a template to a device group. You must apply templates to individual devices in a device group. If you need to apply the same set of templates to multiple devices, you can create a single template that includes all the templates that are to be applied to a device, and then apply the combined template to each device.

For an example of creating a device group, see “Adding Device Groups” in the Network and Security Manager Administration Guide.

**Related Topics**
- About Device Creation on page 23
- Supported Add Device Workflows for M-series and MX-series Devices on page 24
- Importing Devices Overview on page 25
- Modeling Devices Overview on page 26
- Adding Multiple Devices Using Automatic Discovery (JUNOS Software Devices Only) on page 27
Chapter 5
Updating M-series and MX-series Devices
Overview

- About Updating M-series and MX-series Devices on page 29
- How the Update Process Works on page 30
- Job Manager on page 31
- Tracking Updated Devices Using Job Manager on page 32
- Reviewing Job Information Displayed in Job Manager on page 33
- Device States Displayed in Job Manager During Update on page 34
- Understanding Updating Errors Displayed in the Job Manager on page 35

About Updating M-series and MX-series Devices

When you update a managed device, you modify the running device configuration (the configuration currently installed on the physical device) with the modeled device configuration (the configuration currently modeled in Network and Security Manager (NSM)).

You can update a single device, multiple devices, or device groups simultaneously. For example, if you have created a device group that includes only M-series devices, you can update the entire device group in a single update procedure. During the update, NSM displays the progress of the update on each individual device so you can see exactly what is happening. Simultaneous updating also reduces downtime to unaffected devices and areas of your network.

Updating a device is a three-step process.

1. Ensure that you have configured the device correctly, created and assigned a policy to the device, and established a connection between the device and the management server.

2. From the Device Manager launchpad, select Update Device. The launchpad displays the Update Device(s) dialog box.

All connected and managed devices appear in the device list. Modeled devices and devices awaiting import for the first time do not appear.

3. Select the devices or device groups you want to update and click Apply Changes. NSM updates the selected devices or device groups with the modeled configuration.
NSM uses centralized control and tracking to indicate when you need to update a device, and to follow the progress of the device configuration you are updating. Before updating your managed devices, you can use other NSM modules and tools to identify devices that need to be updated, validate their modeled configurations, and preview how those devices accept the new configuration. After updating, you can use the same tools to verify a successful update. These tools include:

- **Audit Log Viewer**—This NSM module records changes made to a device configuration. The audit log entry also identifies the administrator who performed the change, shows when the change was updated on the device, and provides a history of change details.

- **Configuration Summaries**—These tools provide a preview of the modeled configuration, enabling you to compare it with the configuration that is running on the device. Use configuration summaries to ensure the modeled configuration is consistent with what you want to update on the device.

- **Job Manager**—This NSM module tracks the status of running and completed update processes. The Job Manager displays details of the update process in a dedicated information window and includes the update’s success or failure and errors involved in a failed update.

For more information about updating devices, including knowing when to update, using preview tools, performing updates, tracking updates and rebooting devices, see “Updating Devices” in the Network and Security Manager Administration Guide.

### Related Topics
- How the Update Process Works on page 30
- Job Manager on page 31
- Tracking Updated Devices Using Job Manager on page 32
- Reviewing Job Information Displayed in Job Manager on page 33
- Device States Displayed in Job Manager During Update on page 34
- Understanding Updating Errors Displayed in the Job Manager on page 35

### How the Update Process Works

After you have successfully added the device to NSM, reviewed the device configuration, updated the device, and have the managed device functioning normally, an event might occur on the managed device that requires a change to the device configuration. For example, malicious traffic might have entered your network, requiring you to update the device to detect and prevent that attack.

1. Using the NSM monitoring tools, you learn of the attack and locate the cause of the event. Using NSM modules such as the Realtime Monitor and Log Viewer, you determine the exact attack that penetrated the device. From the Report Manager, you also determine what rule in the security policy was ineffective in blocking the attack.

2. You update the modeled device configuration, editing the configuration to detect and prevent the attack from entering your network again.

3. Before updating the running configuration, you review the modeled device configuration. Using a delta configuration summary, compare the modeled
configuration with the running configuration on the device to confirm the differences. Fine-tune the modeled configuration, if needed.

4. When you are confident that the modeled configuration is valid, update the device. NSM updates the running configuration with only the new changes (delta). During the update, you track the update progress using Job Manager in real time and observe the transfer of the configuration from NSM to the device.

If the update is unsuccessful, use the information in the Job information dialog box to correct the problems in the modeled configuration.

5. After updating, run a second delta configuration summary to identify any remaining differences between the modeled configuration and the running configuration on the device. When the delta configuration summary reveals no differences between the new configuration and the old configuration on the device, you have successfully updated the running configuration.

**Related Topics**

- About Updating M-series and MX-series Devices on page 29
- Job Manager on page 31
- Tracking Updated Devices Using Job Manager on page 32
- Reviewing Job Information Displayed in Job Manager on page 33
- Device States Displayed in Job Manager During Update on page 34
- Understanding Updating Errors Displayed in the Job Manager on page 35

**Job Manager**

You can view the progress of communication to and from your devices in the Job Manager, that is located in the Administer panel. NSM sends commands to managed devices at your request, typically to import, update or reboot devices, and view configuration and delta configuration summaries. When you send a command to a device or group of devices, NSM creates a job for that command and displays information about that job in the Job Manager module.

Job Manager tracks the progress of the command as it travels to the device and back to the management system. Each job contains:

- Name of the command
- Date and time the command was sent
- Completion status for each device that received the command
- Detailed description of command progress
- Command output, such as a configuration list or command-line interface (CLI) changes on the device
NOTE: Job Manager configuration summaries and job information details do not display passwords in the list of CLI commands for administrators that do not have the assigned activity “View Device Passwords.” By default, only the super administrator has this assigned activity.

Related Topics
- About Updating M-series and MX-series Devices on page 29
- How the Update Process Works on page 30
- Tracking Updated Devices Using Job Manager on page 32
- Reviewing Job Information Displayed in Job Manager on page 33
- Device States Displayed in Job Manager During Update on page 34
- Understanding Updating Errors Displayed in the Job Manager on page 35

Tracking Updated Devices Using Job Manager

Use Job Manager to track device updates in real time. You can view the status of a running update and the status of completed updates in the Job Manager module.

When you send a command to a device or group of devices using NSM, the management system creates a job for that command and displays information about that job in the Job Information dialog box. The command you send is called a directive.

Job Manager includes the following utilities and information:
- View Controls—Use View controls to set the information level you want displayed in Job Manager:
  - Expand All displays all devices associated with a directive type.
  - Collapse All displays the directive type.
- Job Type (Directive) List—Displays the job type (directives) and associated timestamp completion status information. All current and completed jobs appear, including device updates. However, if you have not yet performed an update using NSM, the Job List does not display an Update Configuration directive.
- Notification Controls—Enables you to manually view job completion status.
- Job Information—Enables you to view job information, including errors, job completion status, job state, automatic job completion notification setting, and start time of job.

Related Topics
- About Updating M-series and MX-series Devices on page 29
- How the Update Process Works on page 30
- Job Manager on page 31
- Reviewing Job Information Displayed in Job Manager on page 33
- Device States Displayed in Job Manager During Update on page 34
- Understanding Updating Errors Displayed in the Job Manager on page 35
Reviewing Job Information Displayed in Job Manager

The Job Information dialog box displays the changing device states as the directive is executed. Device state changes, error messages, and warning messages are displayed in real time. A sample Job Information dialog box is shown in Figure 3 on page 33.

Figure 3: Job Information Dialog Box

Job Manager tracks the overall progress of one or more jobs executed on a single device. For multiple device updates, Job Manager tracks the progress of each job on each device in addition to the overall progress for all devices. To view the job status for an individual device (including error messages and percent complete), select the device in the Percent Complete pane; the status appears in the Output pane.

The job information includes:

- **Job Type**—The type of task being tracked. Job types include Update Device, Reboot Device, and Config Summary. Job type is also known as a directive.
- **Timestamp**—The time at which NSM began executing the directive.
- **Admin Name**—The name of the administrator logged into NSM.
- **Status**—The current state of the job.
- **Completion**—The number of jobs completed out of the total number of jobs.
- **Percent**—The percentage of total jobs successfully executed. When performing multiple jobs on multiple devices, this field displays the percentage complete for each device. When the job has completed, successfully or unsuccessfully, this field displays 100%.
- **Name**—The name of the device on which the job is executed.
- **Description**—The current state of the job.
- **Completion**—The percentage of a job that has executed successfully.
- **Output**—Displays the content of the update, including commands that have been interpreted from the NSM data model into device-specific commands, error messages, and existing commands deleted from the device. The Output Display Region displays all errors, warnings, device verification output, and device state information associated with the job.

**NOTE:** If the Job Information dialog box might contain Chinese, Japanese, or Korean characters, you must uncheck the Fixed Font box to display them.

**NOTE:** Job Manager configuration summaries and job information details do not display passwords in the list of CLI commands for administrators that do not have the assigned activity “View Device Passwords.” By default, only the super administrator has this assigned activity.

**Related Topics**
- About Updating M-series and MX-series Devices on page 29
- How the Update Process Works on page 30
- Job Manager on page 31
- Tracking Updated Devices Using Job Manager on page 32
- Device States Displayed in Job Manager During Update on page 32
- Understanding Updating Errors Displayed in the Job Manager on page 35

### Device States Displayed in Job Manager During Update

During an update, the managed device changes device state. You can view the current device state in real time in the State Description field of the Job Information dialog box. Table 6 on page 34 lists the states that a device can have.

<table>
<thead>
<tr>
<th>Device State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No update activity has occurred on the device.</td>
</tr>
<tr>
<td>Loading in Progress</td>
<td>NSM is sending the update image to the flash memory of the device.</td>
</tr>
<tr>
<td>Pending</td>
<td>Device is accepting the parameters from the update configuration that has been sent to the device flash memory.</td>
</tr>
<tr>
<td>Converting Data Model to Device Data Model</td>
<td>The parameters that have been set in the NSM configuration are being changed to corresponding device-specific CLI commands that execute on the device.</td>
</tr>
</tbody>
</table>
Table 6: Device States During Update (continued)

<table>
<thead>
<tr>
<th>Device State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful Completion</td>
<td>Device has successfully been updated with the modeled configuration.</td>
</tr>
<tr>
<td>Failed</td>
<td>Device has not been successfully updated with the modeled configuration. The Job Information dialog box displays error messages and error codes.</td>
</tr>
</tbody>
</table>

Related Topics

- About Updating M-series and MX-series Devices on page 29
- How the Update Process Works on page 30
- Job Manager on page 31
- Tracking Updated Devices Using Job Manager on page 32
- Reviewing Job Information Displayed in Job Manager on page 33
- Understanding Updating Errors Displayed in the Job Manager on page 35

Understanding Updating Errors Displayed in the Job Manager

When an update fails for any reason, Job Manager displays error codes and error messages that can help you identify and locate the problem. Typical errors include:

- The modeled configuration contained invalid values that the device could not process.
- During the update process, the connection between the managed device and the Device Server was lost.
- The modeled configuration caused the managed device to lose its connection to NSM.
- An exclusive lock on the configuration prevented NSM from completing an update. This error is specific to devices running the Device Management Interface (DMI), such as the M-series and MX-series devices.

For these update errors, the Job Information dialog box displays the job status as “Failed.”

Figure 4 on page 36 shows that on December 4 a configuration update to an MX960 failed. The super user was locked out by the root user as indicated in the text of the error that shows lock Failed and configuration database locked by: root. For an M-series or MX-series device, NSM attempts to acquire an exclusive lock on the candidate configuration so that the update can proceed. In this instance, the root user was updating the configuration, probably from the CLI, preventing NSM from locking and successfully updating the configuration.
In the Job Information dialog box, the update:

- Successfully checked sanity
- Unsuccessfully attempted to lock the configuration that was already locked by the root user

At the end of the error message, there are some suggestions as to how to proceed. In this particular case, the second solution, `> request system logout pid xxxx`, is the appropriate action. From the CLI, the `request system logout pid pid` command can be used to forcibly log out the root user. The root user is represented by `pid pid`, which indicates the user session using the specified management process identifier (PID). After the root user is locked out, you can try to update the configuration again. NSM should lock the configuration and continue successfully.

After a device is updated, you can run a delta configuration summary to determine any remaining differences between the modeled configuration and the running configuration; the output of this summary appears in the Job Information dialog box. For successful updates, no discrepancies are found or displayed. For failed updates, the Job Information dialog box lists the remaining discrepancies.
You can also check the Connection Status and Configuration Status columns for the device in the Realtime Monitor to determine whether the device is running. For more information, see “About the Realtime Monitor.”

**Related Topics**
- About Updating M-series and MX-series Devices on page 29
- How the Update Process Works on page 30
- Job Manager on page 31
- Tracking Updated Devices Using Job Manager on page 32
- Reviewing Job Information Displayed in Job Manager on page 33
- Device States Displayed in Job Manager During Update on page 34
Understanding Updating Errors Displayed in the Job Manager
Part 3
Configuring M-series and MX-series Devices

- Configuring M-series and MX-series Devices Overview on page 41
- Configuring Authentication on page 47
- Configuring Class of Service Features on page 55
- Configuring SNMP on page 75
Chapter 6

Configuring M-series and MX-series Devices Overview

- About Device Configuration on page 41
- M-series and MX-series Device Configuration Settings Supported in NSM on page 42
- Configuring Device Features on page 44
- Example: Configuration of Interfaces for MPLS in the CLI and NSM on page 45

About Device Configuration

This topic does not provide extensive details for configuring features on M-series and MX-series devices in Network and Security Manager (NSM). For detailed information about configuring specific features for M-series and MX-series devices, see the following JUNOS software configuration guide:

- JUNOS System Basics Configuration Guide for system, chassis, security, and access parameters.
- JUNOS Network Interfaces Configuration Guide for interface parameters.
- JUNOS Configuration and Diagnostic Automation Guide for event options parameters.
- JUNOS VPNs Configuration Guide for policy options parameters.
- JUNOS Class of Service Configuration Guide for class of service parameters.
- JUNOS Services Interface Configuration Guide for service parameters.

For more information about editing device configurations in NSM, including using device templates, using configuration groups, and using configuration groups with...
You can configure JUNOS software features in NSM. Although the configuration screens rendered in NSM look different than the JUNOS command-line interface (CLI), the top-level configuration elements mostly correspond to commands in the CLI.

NOTE: For detailed information about configuring specific features for M-series and MX-series devices, see the appropriate JUNOS software configuration guide.

Table 7 on page 42 provides a general guideline of the CLI hierarchy levels that are supported in the NSM configuration tree. For the exact parameters available, double-click the device in the Device Manager and select the Configuration tab. The configuration tree appears in the main display area with all parameters viewable or configurable from NSM.

**Table 7: The JUNOS Configuration Hierarchy and the NSM Configuration Tree**

<table>
<thead>
<tr>
<th>Hierarchy Level</th>
<th>Available in the NSM Configuration Tree</th>
</tr>
</thead>
<tbody>
<tr>
<td>edit access</td>
<td>Yes</td>
</tr>
<tr>
<td>edit accounting-options</td>
<td>Yes</td>
</tr>
<tr>
<td>edit applications</td>
<td>Yes</td>
</tr>
<tr>
<td>edit bridge domains</td>
<td>Yes</td>
</tr>
<tr>
<td>edit chassis</td>
<td>Yes</td>
</tr>
<tr>
<td>edit class-of-service</td>
<td>Yes</td>
</tr>
<tr>
<td>edit dynamic profiles</td>
<td>Yes</td>
</tr>
<tr>
<td>edit ethernet-switching-options</td>
<td>No</td>
</tr>
<tr>
<td>edit event-options</td>
<td>Yes</td>
</tr>
<tr>
<td>edit firewall</td>
<td>Yes</td>
</tr>
<tr>
<td>edit forwarding-options</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Table 7: The JUNOS Configuration Hierarchy and the NSM Configuration Tree (continued)

<table>
<thead>
<tr>
<th>Hierarchy Level</th>
<th>Available in the NSM Configuration Tree</th>
</tr>
</thead>
<tbody>
<tr>
<td>edit groups</td>
<td>Yes</td>
</tr>
<tr>
<td>edit interfaces</td>
<td>Yes</td>
</tr>
<tr>
<td>edit logical-systems</td>
<td>Yes</td>
</tr>
<tr>
<td>edit multicast-snooping-options</td>
<td>Yes</td>
</tr>
<tr>
<td>edit poe</td>
<td>No</td>
</tr>
<tr>
<td>edit policy-options</td>
<td>Yes</td>
</tr>
<tr>
<td>edit protocols</td>
<td>Yes</td>
</tr>
<tr>
<td>edit routing-instances]</td>
<td>Yes</td>
</tr>
<tr>
<td>edit routing-options</td>
<td>Yes</td>
</tr>
<tr>
<td>edit schedulers</td>
<td>No</td>
</tr>
<tr>
<td>edit security</td>
<td>Yes</td>
</tr>
<tr>
<td>edit services</td>
<td>Yes</td>
</tr>
<tr>
<td>edit snmp</td>
<td>Yes</td>
</tr>
<tr>
<td>edit switch-options</td>
<td>Yes</td>
</tr>
<tr>
<td>edit system</td>
<td>Yes</td>
</tr>
<tr>
<td>edit virtual-chassis</td>
<td>No</td>
</tr>
<tr>
<td>edit vlans</td>
<td>No</td>
</tr>
</tbody>
</table>

When you use NSM to edit the software configuration on the device, you initially make the changes to a device object that models the device in NSM. When you are satisfied with your configuration changes, you use the Update Device directive to push the configuration from the device object in NSM to the device itself. At that point, the edited configuration becomes active.

**NOTE:** If you import an existing device configuration, NSM automatically imports all objects defined in that configuration.

For more information about editing device configurations, using device templates, using configuration groups, and using configuration groups with templates, see “Configuring Devices” in the Network and Security Manager Administration Guide.

**Related Topics**
- About Device Configuration on page 41
Configuring Device Features

You can configure JUNOS software features in NSM. Although the configuration screens rendered in NSM look different than the JUNOS command-line interface (CLI), the top-level configuration elements mostly correspond to commands in the CLI.

**NOTE:** For detailed information about configuring specific features for M-series and MX-series devices, see the appropriate JUNOS software configuration guide.

To configure a device that has been added, imported, or modeled in NSM:

1. In the navigation tree, select Device Manager > Devices.
2. Open the device configuration using one of the following methods:
   - Double-click the device object in the security device tree or the device list.
   - Select the device object and then click the Edit icon.
   - Right-click the device object and select Edit.
3. Select the Configuration tab.

   The device configuration tree appears in the left pane.
4. In the device navigation tree, select a function heading to see device parameters, and then select the configuration parameter you want to configure.
5. Make your changes to the device configuration, then choose one of the following:
   - Click OK to save your changes and close the device configuration.
   - Click Apply to save your changes and continue making changes.
   - Click Cancel to discard all changes and close the device configuration.

To reset a device feature to its default value, right-click on the feature name in the device editor and select Revert to template/default value.

Related Topics

- About Device Configuration on page 41
- M-series and MX-series Device Configuration Settings Supported in NSM on page 42
- Example: Configuration of Interfaces for MPLS in the CLI and NSM on page 45
Example: Configuration of Interfaces for MPLS in the CLI and NSM

With NSM you can manage most of the parameters that you can configure through the CLI. Although the configuration screens rendered in NSM look different, the top-level configuration elements essentially correspond to commands in the CLI. You can configure an M-series or MX-series device using the CLI, then import the configuration into NSM to create a template and apply it to multiple devices.

The following figures show the same configuration displayed in the CLI and the NSM UI. Figure 5 on page 45 shows the CLI configuration of MPLS at the `edit protocols mpls` hierarchy level, and Figure 6 on page 46 shows the same configuration in the NSM UI.

Figure 5 on page 45 shows output for the `show` command in configuration mode. At this level, the `show` command typically displays the entire configuration for the device. For the purpose of this illustration, all parts of the configuration not relevant to our example were removed [...Output Truncated...]. The remaining output shows the protocols and MPLS hierarchy levels. Included at the hierarchy level are three interfaces, two Fast Ethernet interfaces (fe) and one Gigabit Ethernet interface (ge).

**Figure 5: MPLS Configuration in the CLI**

```
[edit]
user@host# show
[...Output Truncated...]
protocols {
    mpls {
        interface ge-1/3/0.0;
        interface fe-0/1/2.0;
        interface fe-0/1/1.0;
    }
}
```

Figure 6 on page 46 shows the NSM UI with the same information as in the CLI example. On the left, the Navigation tree is expanded at Protocols, and then further expanded at MPLS, similar to the CLI hierarchy levels. Within MPLS, Interface is highlighted, indicating that the information on the right relates to interfaces within MPLS. The information in the NSM UI example is similar to the information in the CLI example though the presentation is somewhat different.
In addition, Figure 6 on page 46 shows parts of the configuration tree that are grayed out, indicating that those particular parameters are not supported for the M-series and MX-series devices.

Related Topics

- About Device Configuration on page 41
- M-series and MX-series Device Configuration Settings Supported in NSM on page 42
- Configuring Device Features on page 44
Chapter 7
Configuring Authentication

- Configuring RADIUS Authentication (NSM Procedure) on page 47
- Configuring TACACS+ Authentication (NSM Procedure) on page 48
- Configuring Authentication Order (NSM Procedure) on page 49
- Configuring User Access (NSM Procedure) on page 50
- Configuring Template Accounts (NSM Procedure) on page 51

Configuring RADIUS Authentication (NSM Procedure)

To use RADIUS authentication, you must configure at least one RADIUS server. Configuring RADIUS authentication involves identifying the RADIUS server, specifying the secret (password) of the RADIUS server, and setting the source address of the device's RADIUS requests to the loopback address of the device.

To configure RADIUS authentication:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device for which you want to configure RADIUS authentication.
3. Click the Configuration tab. In the configuration tree, select System > Radius Server.
4. Add or modify Radius settings as specified in Table 8 on page 47.
5. Click one:
   - **New**—Adds a new RADIUS server.
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.

Table 8: RADIUS Authentication Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the IP address of the RADIUS server.</td>
<td>Enter the IP address of the RADIUS server.</td>
</tr>
</tbody>
</table>
Table 8: RADIUS Authentication Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secret</td>
<td>Specifies the shared secret (password) of the RADIUS server. The secret is stored as an encrypted value in the configuration database.</td>
<td>Enter the shared secret of the RADIUS server.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Specifies the source address to be included in the RADIUS server requests by the device. In most cases, you can use the loopback address of the device.</td>
<td>Enter the loopback address of the device.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring TACACS+ Authentication (NSM Procedure) on page 48
- Configuring Authentication Order (NSM Procedure) on page 49
- Configuring User Access (NSM Procedure) on page 50

Configuring TACACS+ Authentication (NSM Procedure)

To use TACACS+ authentication, you must configure at least one TACACS+ server. Configuring TACACS+ authentication involves identifying the TACACS+ server, specifying the secret (password) of the TACACS+ server, and setting the source address of the device’s TACACS+ requests to the loopback address of the device.

To configure TACACS+ authentication:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab and then double-click the device for which you want to configure TACACS+ authentication.
3. Click the Configuration tab. In the configuration tree, select System > TACACS+ Server.
4. Add or modify TACACS+ settings as specified in Table 9 on page 48.
5. Click one:
   - New—Adds a new TACACS+ server.
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 9: TACACS+ Authentication Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the IP address of the TACACS+ server.</td>
<td>Enter the IP address of the TACACS+ server.</td>
</tr>
<tr>
<td>Secret</td>
<td>Specifies the shared secret (password) of the TACACS+ server. The secret is stored as an encrypted value in the configuration database.</td>
<td>Enter the shared secret of the TACACS+ server.</td>
</tr>
</tbody>
</table>
Table 9: TACACS+ Authentication Configuration Details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Specifies the source address to be included in the TACACS+ server requests by the device. In most cases, you can use the loopback address of the device.</td>
<td>Enter the loopback address of the device.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring RADIUS Authentication (NSM Procedure) on page 47
- Configuring Authentication Order (NSM Procedure) on page 49
- Configuring User Access (NSM Procedure) on page 50

Configuring Authentication Order (NSM Procedure)

You can configure the device so that user authentication occurs with the local password first, then with the RADIUS server, and finally with the TACACS+ server.

To configure authentication order:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab and then double-click the device for which you want to configure authentication order.
3. Click the Configuration tab. In the configuration tree, select System > Authentication Order.
4. In the Authentication Order workspace, click the New button. The New authentication-order list appears.
5. To add RADIUS authentication to the authentication order, select radius from the New authentication-order list.
6. To add TACACS+ authentication to the authentication order, select tacplus from the New authentication-order list.
7. To add Password authentication to the authentication order, select password from the New authentication-order list.
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Related Topics
- Configuring RADIUS Authentication (NSM Procedure) on page 47
- Configuring TACACS+ Authentication (NSM Procedure) on page 48
- Configuring User Access (NSM Procedure) on page 50
Configuring User Access (NSM Procedure)

This section includes the following topics:

- Configuring Login Classes on page 50
- Configuring User Accounts on page 51

Configuring Login Classes

You can define any number of login classes and then apply one login class to an individual user account. All users who can log in to the router must be in a login class. With login classes, you define the following:

- Access privileges users have when they are logged in to the router
- Commands and statements that users can and cannot specify
- How long a login session can be idle before it times out and the user is logged out

To configure login classes:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab and then double-click the device for which you want to configure a login class.
3. Click the **Configuration** tab. In the configuration tree, select **System > Login > Class**.
4. Add or modify login class settings as specified in Table 10 on page 50.
5. Click one:
   - **New**—Adds a new login class.
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 10: Login Class Authentication Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name for the login class.</td>
<td>Enter a name for the login class.</td>
</tr>
<tr>
<td>Allow Commands</td>
<td>Specifies the operational mode commands that members of a login class can use.</td>
<td>Enter the command name enclosed in quotation marks. For example, “request system reboot”.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Configures the login access privileges to be provided on the device.</td>
<td>Enter a new permission.</td>
</tr>
</tbody>
</table>
Configuring User Accounts

User accounts provide one way for users to access the device. (Users can access the router without accounts if you configured RADIUS or TACACS+ servers.) For each account, define the login name for the user and, optionally, information that identifies the user. After you have created an account, a home directory is created for the user.

To configure user accounts:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab and then double-click the device for which you want to configure login class.
3. Click the Configuration tab. In the configuration tree, select System > Login > User.
4. Add or modify login class settings as specified in Table 11 on page 51.
5. Click one:
   - **New**—Adds a new user account.
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

### Table 11: User Authentication Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identifies the user with a unique name.</td>
<td>Enter a unique name for the user.</td>
</tr>
<tr>
<td>Class</td>
<td>Specifies the user's login class.</td>
<td>Select the class name.</td>
</tr>
</tbody>
</table>

**Login > User > Authentication**

| Plain Text Password Value | Specifies the user’s password. | Enter the plain text password for the user. |

**Related Topics**
- Configuring RADIUS Authentication (NSM Procedure) on page 47
- Configuring TACACS+ Authentication (NSM Procedure) on page 48
- Configuring Authentication Order (NSM Procedure) on page 49

Configuring Template Accounts (NSM Procedure)

You can create template accounts that are shared by a set of users when you are using RADIUS or TACACS+ authentication. When a user is authenticated by a
template account, the CLI username is the login name, and the privileges, file ownership, and effective user ID are inherited from the template account.

To configure template accounts, follow these procedures:
- Creating a Remote Template Account on page 52
- Creating a Local Template Account on page 53

Creating a Remote Template Account

You can create a remote template that is applied to users authenticated by RADIUS or TACACS+ that do not belong to a local template account.

By default, JUNOS software with enhanced services uses the remote template account when:
- The authenticated user does not exist locally on the Services Router.
- The authenticated user's record in the RADIUS or TACACS+ server specifies local user, or the specified local user does not exist locally on the device.

The following procedure creates a sample user named remote that belongs to the operator login class.

To create a remote template account:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab and then double-click the device for which you want to create a remote template account.
3. Click the Configuration tab. In the configuration tree, select System > Login > User.
4. Add or modify login class settings as specified in Table 12 on page 52.
5. Click one:
   - New—Creates a new remote template account.
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 12: Remote Template Account Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name for the user name.</td>
<td>Enter the user name. For example, type remote</td>
</tr>
<tr>
<td>Uid</td>
<td>Specifies the user identifier for a login account.</td>
<td>Enter the number associated with the login account.</td>
</tr>
<tr>
<td>Class</td>
<td>Specifies the login class for the user.</td>
<td>Select the login class. For example, select operator.</td>
</tr>
</tbody>
</table>
**Creating a Local Template Account**

You can create a local template that is applied to users authenticated by RADIUS or TACACS+ that are assigned to the local template account. You use local template accounts when you need different types of templates. Each template can define a different set of permissions appropriate for the group of users who use that template.

The following procedure creates a sample user named admin that belongs to the superuser login class.

To create a local template account:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab and then double-click the device for which you want to create a local template account.
3. Click the **Configuration** tab. In the configuration tree, select **System > Login > User**.
4. Add or modify login class settings as specified in Table 13 on page 53.
5. Click one:
   - **New**—Creates a new local template account.
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

**Table 13: Local Template Account Details**

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name for the user name.</td>
<td>Enter the user name. For example, type <strong>admin</strong>.</td>
</tr>
<tr>
<td>Uid</td>
<td>Specifies the user identifier for a login account.</td>
<td>Enter the number associated with the login account.</td>
</tr>
<tr>
<td>Class</td>
<td>Specifies the login class for the user.</td>
<td>Select the login class. For example, select <strong>superuser</strong>.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring RADIUS Authentication (NSM Procedure) on page 47
- Configuring TACACS+ Authentication (NSM Procedure) on page 48
- Configuring Authentication Order (NSM Procedure) on page 49
Creating a Local Template Account
Packet classification associates incoming packets with a particular class-of-service (Cos) servicing level. Classifiers associate packets with a forwarding class and loss priority and, based on the associated forwarding class, assign packets to output queues. JUNOS software supports two general types of classifiers:

- **Behavior aggregate or CoS value traffic classifiers**—Examines the CoS value in the packet header. The value in this single field determines the CoS settings applied to the packet. BA classifiers allow you to set the forwarding class and loss priority of a packet based on the Differentiated Services code point (DSCP) value, IP precedence value, and IEEE 802.1p value. The default classifier is based on the DSCP value.

- **Multifield traffic classifiers**—Examines multiple fields in the packet such as source and destination addresses and source and destination port numbers of the packet. With multifield classifiers, you set the forwarding class and loss priority of a packet based on firewall filter rules.

To configure and apply behavior aggregate classifiers for the switch:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure and apply behavior aggregate classifiers.
3. Click the **Configuration** tab. In the configuration tree expand **Class of Service**.
4. Select **Classifiers**.
5. Add or modify settings as specified in Table 14 on page 56.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

**NOTE:** After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the Network and Security Manager Administration Guide for more information.

Table 14: Configuring and Applying Behavior Aggregate Classifiers

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure behavior aggregate classifiers for DiffServ CoS.</td>
<td>1. Click Add new entry next to Dscp.</td>
</tr>
<tr>
<td></td>
<td>2. In the Name box, type the name of the behavior aggregate classifier—for example, ba-classifier.</td>
</tr>
<tr>
<td></td>
<td>3. In the Import box, type the name of the default DSCP map.</td>
</tr>
<tr>
<td>Configure a best-effort forwarding class classifier.</td>
<td>1. Click Add new entry next to Forwarding class.</td>
</tr>
<tr>
<td></td>
<td>2. In the Class name box, type the name of the previously configured best-effort forwarding class—for example, be-class.</td>
</tr>
<tr>
<td></td>
<td>3. Click Add new entry next to Loss priority.</td>
</tr>
<tr>
<td></td>
<td>4. From the Loss val list, select high.</td>
</tr>
<tr>
<td></td>
<td>5. Click Add new entry next to Code points.</td>
</tr>
<tr>
<td></td>
<td>6. In the Value box, type the value of the high-priority code point for best-effort traffic—for example, 00001.</td>
</tr>
<tr>
<td></td>
<td>7. Click OK three times.</td>
</tr>
<tr>
<td>Configure an expedited forwarding class classifier.</td>
<td>1. Click Add new entry next to Forwarding class.</td>
</tr>
<tr>
<td></td>
<td>2. In the Class name box, type the name of the previously configured expedited forwarding—for example, class-ef-class.</td>
</tr>
<tr>
<td></td>
<td>3. Click Add new entry next to Loss priority.</td>
</tr>
<tr>
<td></td>
<td>4. From the Loss val list, select high.</td>
</tr>
<tr>
<td></td>
<td>5. Click Add new entry next to Code points.</td>
</tr>
<tr>
<td></td>
<td>6. In the Value box, type the value of the high-priority code point for expedited forwarding traffic—for example, 101111.</td>
</tr>
<tr>
<td></td>
<td>7. Click OK three times.</td>
</tr>
</tbody>
</table>
Table 14: Configuring and Applying Behavior Aggregate Classifiers (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
| Configure an assured forwarding class classifier. | 1. Click **Add new entry** next to Forwarding class.  
2. In the Class name box, type the name of the previously configured assured forwarding—for example, **class-af-class**.  
3. Click **Add new entry** next to Loss priority.  
4. From the Loss val list, select **high**.  
5. Click **Add new entry** next to Code points.  
6. In the Value box, type the value of the high-priority code point for assured forwarding traffic—for example, **001100**.  
7. Click **OK** three times. |

| Apply the behavior aggregate classifier to an interface. | 1. Click **Add new entry** next to Interfaces.  
2. In the Interface name box, type the name of the interface—for example, **ge-0/0/0**.  
3. Click **Add new entry** next to Unit.  
4. In the Unit number box, type the logical interface unit number—for example, **0**.  
5. Click **Configure** next to Classifiers.  
6. In the Classifiers box, under Dscp, type the name of the previously configured behavior aggregate classifier—for example, **ba-classifier**.  
7. Click **OK**. |

Related Topics

- Configuring CoS Code Point Aliases (NSM Procedure) on page 57
- Configuring CoS Drop Profile (NSM Procedure) on page 59
- Configuring CoS Forwarding Classes (NSM Procedure) on page 61
- Configuring CoS Interfaces (NSM Procedure) on page 62
- Configuring CoS Rewrite Rules (NSM Procedure) on page 68
- Configuring CoS Schedulers (NSM Procedure) on page 71
- Configuring CoS and Applying Scheduler Maps on page 72

### Configuring CoS Code Point Aliases (NSM Procedure)

You can use code-point aliases to streamline the process of configuring CoS features on your device. A code-point alias assigns a name to a pattern of code-point bits. You can use this name instead of the bit pattern when you configure other CoS components such as classifiers, drop-profile maps, and rewrite rules.

To configure code-point aliases:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure CoS code point aliases.
3. Click the Configuration tab. In the configuration tree, expand Class of Service.
4. Select Code Point Aliases.
5. Add or modify the settings as specified in Table 15 on page 58
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

**NOTE:** After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the Network and Security Manager Administration Guide for more information.

**Table 15: Configuring Code Point Aliases**

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign an alias to the dscp code point</td>
<td>1. In the Configuration tree, expand Code Point Aliases.</td>
</tr>
<tr>
<td></td>
<td>2. Select Dscp</td>
</tr>
<tr>
<td></td>
<td>3. Click the Add New icon.</td>
</tr>
<tr>
<td></td>
<td>4. In the Name box, type the alias that you want to assign to the code point—for example, my1</td>
</tr>
<tr>
<td></td>
<td>5. In the Bits box, type the code point—for example, 110001</td>
</tr>
<tr>
<td></td>
<td>6. Click OK</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 55
- Configuring CoS Drop Profile (NSM Procedure) on page 59
- Configuring CoS Forwarding Classes (NSM Procedure) on page 61
- Configuring CoS Interfaces (NSM Procedure) on page 62
- Configuring CoS Rewrite Rules (NSM Procedure) on page 68
- Configuring CoS Schedulers (NSM Procedure) on page 71
- Configuring CoS and Applying Scheduler Maps on page 72
Configuring CoS Drop Profile (NSM Procedure)

Drop profiles provide a congestion management mechanism that enables a switch or routing platform to drop the arriving packets when queue buffers become full or begin to overflow. Drop profiles define the meanings of loss priorities. When you configure drop profiles you are essentially setting the value for queue fullness. The queue fullness represents the percentage of the memory used to store packets in relation to the total amount of memory that has been allocated for that specific queue. The queue fullness defines the delay-buffer bandwidth, which provides packet buffer space to absorb burst traffic up to the specified duration of delay. Once the specified delay buffer becomes full, packets with 100 percent drop probability are dropped from the tail of the buffer.

You specify drop probabilities in the drop profile section of the CoS configuration hierarchy and reference them in each scheduler configuration. By default, if you do not configure any drop profile then the drop profile that is in effect functions as the primary mechanism for managing congestion. In the default tail drop profile, when the fill level is 0 percent, the drop probability is 0 percent. When the fill level is 100 percent, the drop probability is 100 percent.

To configure drop profiles in NSM:

1. In the navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device for which you want to configure drop profiles.
3. Click the Configuration tab. In the configuration tree expand Class of Service.
4. Select Drop Profiles.
5. Add or modify the drop profiles as specified in Table 16 on page 59.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See Updating Devices section in the Network and Security Manager Administration Guide for more information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drop Profile</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 16: Drop Profile Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Specifies the drop profile name.</td>
<td>1. Click the <strong>New</strong> button or <strong>Edit</strong> button in the Drop Profile interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the drop profile name in the Name box.</td>
</tr>
<tr>
<td><strong>Comment</strong></td>
<td>Specifies the comment for the drop profile.</td>
<td>1. Click the <strong>New</strong> button or <strong>Edit</strong> button in the Drop Profile interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the comment for the drop profile in the Comment box.</td>
</tr>
</tbody>
</table>

#### Fill Level

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Specifies the fill level for the drop profile.</td>
<td>1. On Drop Profile interface click the <strong>New</strong> button or select a profile and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand the Drop Profile tree and select Fill Level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click the <strong>New</strong> button or select a fill level and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Select a value from Name list.</td>
</tr>
<tr>
<td><strong>Comment</strong></td>
<td>Specifies the comment for the fill level</td>
<td>1. On the Drop Profile interface click the <strong>New</strong> button or select a profile and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand the Drop Profile tree and select Fill Level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click the <strong>New</strong> button or select a fill level and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Enter a comment in the Comment box.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 55
- Configuring CoS Code Point Aliases (NSM Procedure) on page 57
- Configuring CoS Forwarding Classes (NSM Procedure) on page 61
- Configuring CoS Interfaces (NSM Procedure) on page 62
- Configuring CoS Rewrite Rules (NSM Procedure) on page 68
- Configuring CoS Schedulers (NSM Procedure) on page 71
- Configuring CoS and Applying Scheduler Maps on page 72
Configuring CoS Forwarding Classes (NSM Procedure)

Forwarding classes allow you to group packets for transmission. Based on forwarding classes, you assign packets to output queues.

By default, four categories of forwarding classes are defined: best effort, assured forwarding, expedited forwarding, and network control.

**NOTE:** EX-series switches support up to 16 forwarding classes.

To configure CoS forwarding classes:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure CoS forwarding classes.
3. Click the **Configuration** tab. In the configuration tree, expand **Class of Service**.
4. Select **Forwarding Classes**.
5. Add or modify settings as specified in Table 17 on page 61.
6. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

**NOTE:** After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Network and Security Manager Administration Guide* for more information.

### Table 17: Assigning Forwarding Classes to Output Queues

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
| Assign best-effort traffic to queue 0. | 1. Select Queue and click Add new entry.  
                                          2. In the Queue num box, type 0.  
                                          3. In the Class name box, type the previously configured name of the best-effort class—for example, be-class.  
                                          4. Click OK. |
### Configuring CoS Interfaces (NSM Procedure)

An interface is configured for optimal performance in a high-traffic network. This feature enables you to configure interface-specific CoS properties for incoming packets.

To configure CoS interfaces in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device for which you want to configure CoS interfaces.
3. Click the **Configuration** tab. In the configuration tree, expand **Class of Service**.
4. Select **Interfaces**.
5. Add or modify the interfaces as specified in Table 18 on page 63.
6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.
NOTE: After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Network and Security Manager Administration Guide* for more information.

Table 18: Interfaces Configuration Fields

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the interface name.</td>
<td>1. Expand the <strong>Interfaces</strong> tree and select <strong>Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in <strong>Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the interface name in the <strong>Name</strong> box.</td>
</tr>
<tr>
<td>Comment</td>
<td>Specifies the comment for the interface.</td>
<td>1. Expand the <strong>Interfaces</strong> tree and select <strong>Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in <strong>Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the comment for the interface in the <strong>Comment</strong> box.</td>
</tr>
<tr>
<td>Scheduler Map</td>
<td>Specifies the scheduler configuration mapped to the forwarding class.</td>
<td>1. Expand the <strong>Interfaces</strong> tree and select <strong>Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in <strong>Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Select the scheduler map from the list.</td>
</tr>
<tr>
<td>Scheduler Map Chassis</td>
<td>Specifies the scheduler configuration mapped to the forwarding class for the particular chassis in the chassis queue.</td>
<td>1. Expand the <strong>Interfaces</strong> tree and select <strong>Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in <strong>Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Select the scheduler map chassis from the list.</td>
</tr>
<tr>
<td>Option</td>
<td>Function</td>
<td>Your Action</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Input Traffic Control Profile</td>
<td>Applies an input traffic scheduling and shaping profile to the logical interface.</td>
<td>1. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in Interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand the Interface tree and select <strong>Input Traffic Control Profile</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the comment and the profile name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <strong>Ok</strong>.</td>
</tr>
<tr>
<td>Input Traffic Control Profile Remaining</td>
<td>Applies an input traffic scheduling and shaping profile for remaining traffic to the logical interface.</td>
<td>1. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in Interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand the Interface tree and select <strong>Input Traffic Control Profile Remaining</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify a comment and a profile name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <strong>Ok</strong>.</td>
</tr>
<tr>
<td>Output Traffic Control Profile</td>
<td>Applies an output traffic scheduling and shaping profile to the logical interface.</td>
<td>1. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in Interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand the Interface tree and select <strong>Output Traffic Control Profile</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify a comment and a profile name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <strong>Ok</strong>.</td>
</tr>
<tr>
<td>Output Traffic Control Profile Remaining</td>
<td>Applies an output traffic scheduling and shaping profile for remaining traffic to the logical interface.</td>
<td>1. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in Interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Expand the Interface tree and select <strong>Output Traffic Control Profile Remaining</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify a comment and a profile name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <strong>Ok</strong>.</td>
</tr>
</tbody>
</table>
### Table 18: Interfaces Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Shaping Rate  | Shapes the output of the physical interface, so that the interface transmits less traffic than it is physically capable of carrying. | 1. Click the **New** button or select an interface and click the **Edit** button in Interface.  
2. Expand **Interface** tree and select **Shaping Rate**.  
3. Specify the comment and the rate  
4. Click **Ok**. |
| Unit          | Sets the units that need to be allocated to the specific forwarding class and scheduling map. | 1. Click the **New** button or select an interface and click the **Edit** button in Interface.  
2. Expand **Interface** tree and select **Unit**.  
3. Specify the Unit, Classifiers, Output Traffic Control Profile and Shaping Rate.  
4. Click **Ok**. |
| Interface Set | Specifies the interface set name.                                          | 1. Expand the **Interfaces** tree and select **Interface Set**.  
2. Click the **New** button or select an interface set and click the **Edit** button.  
3. Select the name from the list. |
| Name          | Specifies the comment for the interface.                                   | 1. Expand the **Interfaces** tree and select **Interface Set**.  
2. Click the **New** button or select an interface set and click the **Edit** button.  
3. Enter the comment. |
| Comment       | Specifies the comment for the interface.                                   | 1. Expand the **Interfaces** tree and select **Interface Set**.  
2. Click the **New** button or select an interface set and click the **Edit** button.  
3. Enter the comment. |
| Internal Node | Sets the scheduler node as internal, allowing resource scheduling to be applied equally to interface sets that include child nodes and those that do not include child nodes. | 1. Expand the **Interfaces** tree and select **Interface Set**.  
2. Click the **New** button or select an interface set and click the **Edit** button.  
3. Set the internal node. |
Table 18: Interfaces Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Excess Bandwidth Share        | Sets the excess bandwidth sharing value.                                  | 1. Expand the Interfaces tree and select Interface Set.  
2. Click the New button or select an interface set and click the Edit button.  
3. Expand interface—set tree and select Excess Bandwidth Share.  
4. Specify the comment and proportion.  
5. Click Ok.                                                                                                      |
| Input Excess Bandwidth Share  | Sets the excess input bandwidth sharing value.                           | 1. Expand the Interfaces tree and select Interface Set.  
2. Click the New button or select an interface set and click the Edit button.  
3. Expand interface—set tree and select Input Excess Bandwidth Share.  
4. Specify the comment and proportion.  
5. Click Ok.                                                                                                      |
| Input Traffic Control Profile | Applies an input traffic scheduling and shaping profile to the logical interface. | 1. Expand the Interfaces tree and select Interface Set.  
2. Click the New button or select an interface set and click the Edit button.  
4. Specify the comment and profile name.  
5. Click Ok.                                                                                                      |
| Input Traffic Control Profile Remaining | Applies an input traffic scheduling and shaping profile for remaining traffic to the logical interface. | 1. Expand the Interfaces tree and select Interface Set.  
2. Click the New button or select an interface set and click the Edit button.  
3. Expand interface—set tree and select Input Traffic Control Profile Remaining.  
4. Specify the comment and profile name.  
5. Click Ok.                                                                                                      |
Table 18: Interfaces Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Traffic Control Profile</td>
<td>Applies an output traffic scheduling and shaping profile to the logical interface.</td>
<td>1. Expand the Interfaces tree and select Interface Set.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the New button or select an interface set and click the Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Specify the comment and profile name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Click Ok.</td>
</tr>
<tr>
<td>Output Traffic Control Profile</td>
<td>Applies an output traffic scheduling and shaping profile for remaining traffic to the logical interface.</td>
<td>1. Expand the Interfaces tree and select Interface Set.</td>
</tr>
<tr>
<td>Remaining</td>
<td></td>
<td>2. Click the New button or select an interface set and click the Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Expand interface—set tree and select Output Traffic Control Profile Remaining.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Specify the comment and profile name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Click Ok.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 55
- Configuring CoS Code Point Aliases (NSM Procedure) on page 57
- Configuring CoS Drop Profile (NSM Procedure) on page 59
- Configuring CoS Forwarding Classes (NSM Procedure) on page 61
- Configuring CoS Rewrite Rules (NSM Procedure) on page 68
- Configuring CoS Schedulers (NSM Procedure) on page 71
- Configuring CoS and Applying Scheduler Maps on page 72
Configuring CoS Rewrite Rules (NSM Procedure)

You configure rewrite rules to alter CoS values in outgoing packets on the outbound interfaces of a device to match the policies of a targeted peer. Policy matching allows the downstream router in a neighboring network to classify each packet into the appropriate service group.

In addition, you often need to rewrite a given marker such as IP precedence, DSCP, or IEEE 802.1p at the switch's inbound interfaces to accommodate behavior aggregate (BA) classification by core devices.

You do not need to explicitly apply rewrite rules to interfaces. By default, rewrite rules are applied to routed packets.

To configure CoS rewrite rules:
1. In the navigation tree, select Device Manager > Devices
2. Click the Device Tree tab, and then double-click the device for which you want to configure CoS rewrite rules.
3. Click the Configuration tab. In the configuration tree, expand Class of Service
4. Select Rewrite Rules.
5. Add or modify settings as specified in Table 19 on page 68.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

**NOTE:** After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the Network and Security Manager Administration Guide for more information.

### Table 19: Configuring and Applying Rewrite Rules

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure rewrite rules for DiffServ CoS</td>
<td>1. Click Configure next to Rewrite Rules.</td>
</tr>
<tr>
<td></td>
<td>2. Click Add new entry next to Dscp.</td>
</tr>
<tr>
<td></td>
<td>3. In the Name box, type the name of the rewrite rules—for example, rewrite-dscps.</td>
</tr>
</tbody>
</table>
### Table 19: Configuring and Applying Rewrite Rules (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
| Configure best-effort forwarding class rewrite rules. | 1. Click **Add new entry** next to Forwarding class.  
2. In the Queue num box, type **1**.  
3. In the Class name box, type the name of the previously configured best-effort forwarding class—for example, **be-class**.  
4. Click **Add new entry** next to Loss priority.  
5. From the Loss val list, select **low**.  
6. In the Code point box, type the value of the low-priority code point for best-effort traffic—for example, **000000**.  
7. Click **OK**.  
8. Click **Add new entry** next to Loss priority.  
9. From the Loss val list, select **high**.  
10. In the Code point box, type the value of the high-priority code point for best-effort traffic—for example, **000001**.  
11. Click **OK** twice. |
| Configure expedited forwarding class rewrite rules. | 1. Click **Add new entry** next to Forwarding class.  
2. In the Class name box, type the name of the previously configured expedited forwarding class—for example, **ef-class**.  
3. Click **Add new entry** next to Loss priority.  
4. From the Loss val list, select **low**.  
5. In the Code point box, type the value of the low-priority code point for expedited forwarding traffic—for example, **101110**.  
6. Click **OK**.  
7. Click **Add new entry** next to Loss priority.  
8. From the Loss val list, select **high**.  
9. In the Code point box, type the value of the high-priority code point for expedited forwarding traffic—for example, **101111**.  
10. Click **OK** twice. |
Table 19: Configuring and Applying Rewrite Rules (continued)

Configure assured forwarding class rewrite rules.

1. Click **Add new entry** next to Forwarding class.
2. In the Class name box, type the name of the previously configured expedited forwarding class—for example, **af-class**.
3. Click **Add new entry** next to Loss priority.
4. From the Loss val list, select **low**.
5. In the Code point box, type the value of the low-priority code point for assured forwarding traffic—for example, **001010**.
6. Click **OK**.
7. Click **Add new entry** next to Loss priority.
8. From the Loss val list, select **high**.
9. In the Code point box, type the value of the high-priority code point for assured forwarding traffic—for example, **001100**.
10. Click **OK** twice.

Apply rewrite rules to an interface.

1. Click **Add new entry** next to Interfaces.
2. In the Interface name box, type the name of the interface—for example, **ge-0/0/0**.
3. Click **Add new entry** next to Unit.
4. In the Unit number box, type the logical interface unit number—for example, **0**.
5. Click **Configure** next to Rewrite rules.
6. In the Rewrite rules name box, under Dscp, type the name of the previously configured rewrite rules—for example, **rewrite-dscps**.
7. Click **OK**.

Related Topics

- Configuring CoS Classifiers (NSM Procedure) on page 55
- Configuring CoS Code Point Aliases (NSM Procedure) on page 57
- Configuring CoS Drop Profile (NSM Procedure) on page 59
- Configuring CoS Forwarding Classes (NSM Procedure) on page 61
- Configuring CoS Interfaces (NSM Procedure) on page 62
- Configuring CoS Schedulers (NSM Procedure) on page 71
- Configuring CoS and Applying Scheduler Maps on page 72
Configuring CoS Schedulers (NSM Procedure)

Using schedulers, you can assign attributes to queues and thereby provide congestion control for a particular class of traffic. These attributes include the amount of interface bandwidth, memory buffer size, transmit rate, and schedule priority.

To configure CoS schedulers:

1. In the navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device for which you want to configure CoS schedulers.
3. Click the Configuration tab. In the configuration tree expand Class of Service.
4. Select Schedulers.
5. Add or modify the settings as specified in Table 20 on page 71.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

**NOTE:** After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the Network and Security Manager Administration Guide for more information.

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the buffer size.</td>
<td>1. Click the Add New icon.</td>
</tr>
<tr>
<td></td>
<td>2. Expand Buffer Size.</td>
</tr>
<tr>
<td></td>
<td>3. Select Percent.</td>
</tr>
<tr>
<td></td>
<td>4. Under Percent, select the appropriate option:</td>
</tr>
<tr>
<td></td>
<td>- To specify no buffer size, select None.</td>
</tr>
<tr>
<td></td>
<td>- To specify buffer size as a percentage of the total buffer, select percent and type an integer from 1 through 100.</td>
</tr>
<tr>
<td></td>
<td>- To specify buffer size as the remaining available buffer, select remainder.</td>
</tr>
<tr>
<td></td>
<td>5. Click OK</td>
</tr>
</tbody>
</table>
Table 20: Configuring Schedulers (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
| Configure drop profile map. | 1. Click the Add New icon.  
2. Select drop-profile-map.  
3. In the Loss Priority box, select the required loss priority—for example, high.  
4. In the Protocol box, select the type of protocol—for example, any.  
5. In the Drop Profile box, select the previously configured drop profile.  
6. Click OK. |

Specify the transmit rate. | 1. Click the Add New icon.  
2. Expand Transmit Rate.  
3. Select Rate.  
4. Under Rate, select the appropriate option:  
   - To not specify transmit rate, select None.  
   - To enforce a specific transmission rate, select rate and type the transmission rate that you want to enforce.  
   - To specify a percentage of transmission capacity, select percent and type an integer from 1 through 100.  
   - To specify the remaining transmission capacity, select remainder.  
5. Click OK. |

Related Topics |  
Configuring CoS Classifiers (NSM Procedure) on page 55  
Configuring CoS Code Point Aliases (NSM Procedure) on page 57  
Configuring CoS Drop Profile (NSM Procedure) on page 59  
Configuring CoS Forwarding Classes (NSM Procedure) on page 61  
Configuring CoS Interfaces (NSM Procedure) on page 62  
Configuring CoS Rewrite Rules (NSM Procedure) on page 68  
Configuring CoS and Applying Scheduler Maps on page 72 |

Configuring CoS and Applying Scheduler Maps

You associate the schedulers with forwarding classes by means of scheduler maps. You can then associate each scheduler map with an interface, thereby configuring the queues and packet schedulers that operate according to this mapping.

To configure CoS and apply scheduler maps:
1. In the navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device for which you want to configure CoS and apply scheduler maps.
3. Click the Configuration tab. In the configuration tree expand Class of Service.
4. Select Scheduler Maps.
5. Add or modify settings as specified in Table 21 on page 73.
6. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

**NOTE:** After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the Network and Security Manager Administration Guide for more information.

### Table 21: Assigning Forwarding Classes to Output Queues

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
| Configure a scheduler map for DiffServ CoS | 1. Click Add new entry.  
2. In the Name box, type the name of the scheduler map—for example, diffserv-cos-map. |
| Configure a best-effort forwarding class and scheduler. | 1. Select Forwarding Class and click Add new entry.  
2. In the Name box, type the name of the previously configured best-effort forwarding class—for example, be-class.  
3. Select the previously configured best-effort scheduler—for example, be-scheduler.  
4. Click OK. |
| Configure an expedited forwarding class and scheduler. | 1. Select Forwarding Class and click Add new entry.  
2. In the Name box, type the name of the previously configured expedited forwarding class—for example, ef-class.  
3. Select the previously configured expedited forwarding scheduler—for example, ef-scheduler.  
4. Click OK. |
| Configure an assured forwarding class and scheduler. | 1. Select Forwarding Class and click Add new entry.  
2. In the Name box, type the name of the previously configured assured forwarding class—for example, af-class.  
3. Select the previously configured assured forwarding scheduler—for example, af-scheduler.  
4. Click OK. |
Table 21: Assigning Forwarding Classes to Output Queues *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
| Apply the scheduler map to an interface. | 1. Select **Interfaces > Interface** and click **Add new entry**.  
2. In the Interface name box, type the name of the interface—for example, `ge-0/0/0`.  
3. Select **Unit** and click **Add new entry**.  
4. In the Unit name box, select the logical interface unit number—for example, 0.  
5. In the Scheduler map box, type the name of the previously configured scheduler map—for example, `diffserv-cos-map`.  
6. Click **OK**. |

**Related Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 55
- Configuring CoS Code Point Aliases (NSM Procedure) on page 57
- Configuring CoS Drop Profile (NSM Procedure) on page 59
- Configuring CoS Forwarding Classes (NSM Procedure) on page 61
- Configuring CoS Interfaces (NSM Procedure) on page 62
- Configuring CoS Rewrite Rules (NSM Procedure) on page 68
- Configuring CoS Schedulers (NSM Procedure) on page 71
Chapter 9

Configuring SNMP

- Configuring Basic System Identification for SNMP (NSM Procedure) on page 75
- Configuring SNMP Agents and Communities (NSM Procedure) on page 76
- Configuring SNMP Trap Groups (NSM Procedure) on page 77
- Configuring SNMP Views (NSM Procedure) on page 78

Configuring Basic System Identification for SNMP (NSM Procedure)

To configure basic system identification information for SNMP:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab and then double-click the device for which you want to configure basic system identification information.
3. Click the Configuration tab. In the configuration tree, select Snmp.
4. Add or modify basic system identification information as specified in Table 22 on page 75.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 22: Basic System Identification Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td>Specifies a system name for the device.</td>
<td>Enter the system name as a free-form text string.</td>
</tr>
<tr>
<td>Description</td>
<td>Provides a description for the system.</td>
<td>Enter a description for the system. For example, type J4350 with 4 PIMs.</td>
</tr>
<tr>
<td>Location</td>
<td>Specifies the system location information.</td>
<td>Enter the system location information (such as a lab name and a rack name).</td>
</tr>
<tr>
<td>Contact</td>
<td>Specifies the contact information for the system.</td>
<td>Enter the system contact information (such as a name and a phone number).</td>
</tr>
</tbody>
</table>

**Snmp > Engine Id**
Table 22: Basic System Identification Details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Mac Address</td>
<td>Sets the engine ID to use the MAC address.</td>
<td>Select this option.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring SNMP Agents and Communities (NSM Procedure) on page 76
- Configuring SNMP Trap Groups (NSM Procedure) on page 77
- Configuring SNMP Views (NSM Procedure) on page 78

Configuring SNMP Agents and Communities (NSM Procedure)

To configure SNMP agents and communities:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab and then double-click the device for which you want to configure SNMP agents and communities.
3. Click the **Configuration** tab. In the configuration tree, select **Snmp > Community**.
4. Add or modify community and client information as specified in Table 23 on page 76.
5. Click one:
   - **New**—Creates a new community.
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 23: SNMP Agents and Community Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name for the community.</td>
<td>Enter a name for the community.</td>
</tr>
<tr>
<td>View</td>
<td>Specifies the view associated with the community.</td>
<td>Enter the view name.</td>
</tr>
<tr>
<td>Authorization</td>
<td>Specifies the access granted to the community.</td>
<td>Select an access to be granted for the community. For example, type <strong>read-write</strong>.</td>
</tr>
</tbody>
</table>

**SNMP > Community > Client List Name**

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies community access to a client at a particular IP address.</td>
<td>Enter the IP address.</td>
</tr>
</tbody>
</table>
Table 23: SNMP Agents and Community Configuration Details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrict</td>
<td>Restricts client access to the specified IP address.</td>
<td>Select this option to restrict client access for the specified IP address.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring Basic System Identification for SNMP (NSM Procedure) on page 75
- Configuring SNMP Trap Groups (NSM Procedure) on page 77
- Configuring SNMP Views (NSM Procedure) on page 78

Configuring SNMP Trap Groups (NSM Procedure)

To configure trap groups:
1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab and then double-click the device for which you want to configure SNMP trap groups.
3. Click the Configuration tab. In the configuration tree, select Snmp > Trap Group.
4. Add or modify SNMP trap group as specified in Table 24 on page 77.
5. Click one:
   - **New**—Creates a new SNMP trap group.
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 24: SNMP Trap Group Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name for the trap group.</td>
<td>Enter a name for the trap group.</td>
</tr>
<tr>
<td>Version</td>
<td>Specifies the version number of SNMP traps.</td>
<td>Select the version number for the SNMP trap.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Specifies the SNMP trap port number.</td>
<td>Enter the trap port number.</td>
</tr>
<tr>
<td>Routing Instance</td>
<td>Specifies a routing instance for trap targets.</td>
<td>Enter the name of the routing instance.</td>
</tr>
</tbody>
</table>

Snmp > Trap Group > Categories

| Category     | Define the types of traps that will be sent to the targets of the named trap group. | Select the trap type. |

Configuring SNMP Trap Groups (NSM Procedure)
Table 24: SNMP Trap Group Configuration Details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snmp &gt; Trap Group &gt; Targets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the IPv4 or IPv6 address of the system to receive traps.</td>
<td>Enter the IPv4 or IPv6 address of the system, but not a hostname.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring Basic System Identification for SNMP (NSM Procedure) on page 75
- Configuring SNMP Agents and Communities (NSM Procedure) on page 76
- Configuring SNMP Views (NSM Procedure) on page 78

Configuring SNMP Views (NSM Procedure)

To configure SNMP views:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab and then double-click the device for which you want to configure SNMP views.
3. Click the Configuration tab. In the configuration tree, select Snmp > View.
4. Add or modify SNMP views as specified in Table 25 on page 78.
5. Click one:
   - New—Creates a new view.
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Table 25: SNMP View Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name for the view.</td>
<td>Enter a name for the view.</td>
</tr>
<tr>
<td>Snmp &gt; View &gt; Oid</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the MIB for the view.</td>
<td>Enter the OID of the MIB in either dotted integer or subtree name format.</td>
</tr>
<tr>
<td>Include or Exclude</td>
<td>Specifies whether the view includes or excludes the MIB</td>
<td>Select this option.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring Basic System Identification for SNMP (NSM Procedure) on page 75
- Configuring SNMP Agents and Communities (NSM Procedure) on page 76
- Configuring SNMP Trap Groups (NSM Procedure) on page 77
Part 4
Managing M-series and MX-series Devices

■ Managing M-series and MX-series Devices Overview on page 81
■ Viewing the M-series and MX-series Device Inventory in NSM and the CLI on page 83
■ Topology Manager on page 89
Chapter 10
Managing M-series and MX-series Devices
Overview

■ Managing M-series and MX-series Device Software Versions on page 81

Managing M-series and MX-series Device Software Versions

You can use Network and Security Manager (NSM) to upgrade or adjust the software on managed M-series and MX-series devices running JUNOS Release 9.3 or later.

When a software upgrade is applied to an M-series or MX-series device with dual Routing Engines, the upgraded software is applied to both Routing Engines. The backup is upgraded first. The router then reboots and the backup becomes the master. Then the former master is upgraded, as is the standard procedure for upgrading M-series and MX-series devices with dual Routing Engines.

For more information and steps about updating the device software version, see “Upgrading the Device Software” in the Network and Security Manager Administration Guide.

Related Topics
■ Viewing and Reconciling Device Inventory on page 83
■ Comparing Device Inventory in NSM and the CLI on page 84
Viewing the M-series and MX-series Device Inventory in NSM and the CLI

- Viewing and Reconciling Device Inventory on page 83
- Comparing Device Inventory in NSM and the CLI on page 84

Viewing and Reconciling Device Inventory

Device inventory management in Network and Security Manager (NSM) allows you to display information about the hardware, software, and license components of each device. It also provides features to update the NSM database with the most current inventory information from the device. In addition, you can use Device Monitor, Device List, and the device tooltip to view the status of inventory synchronization.

These inventory management features are available for all M-series and MX-series devices. You can use these features to make the NSM database match the device inventory, but you cannot write new inventory information to the device.

Initially, the device inventory in the NSM database is generated when the device is first imported into NSM. Immediately after import, the device inventory in the NSM database matches exactly the inventory on the device itself.

If the hardware on the device is changed, the software is upgraded through the WebUI or CLI, new software packages are installed, and then the inventory on the device is no longer synchronized with the NSM database.

The Device Monitor, Device List, and tooltip shows the hardware and software inventory status for each device. Possible states include:

- In Sync—Inventory in the NSM database matches the device.
- Out of Sync—Inventory in the NSM database does not match the device.
- N/A—Either the device is not yet connected and managed by NSM, or the device is a ScreenOS security device or IDP sensor

Changes to the device inventory are not automatically updated in the NSM database.
For detailed information about comparing and reconciling device inventory, see the Network and Security Manager Administration Guide.

Related Topics
- Managing M-series and MX-series Device Software Versions on page 81
- Comparing Device Inventory in NSM and the CLI on page 84

Comparing Device Inventory in NSM and the CLI

NSM and the JUNOS command-line interface (CLI) display similar information about the device inventory, although screens rendered in NSM look different than the JUNOS CLI. This topic provides an introduction to viewing software and hardware inventory using NSM and compares the NSM view with the CLI output for the same device.

- Viewing Device Inventory in NSM on page 84
- Viewing Device Inventory from the CLI on page 86

Viewing Device Inventory in NSM

**Purpose**
NSM displays the hardware and software inventory for each device according to the information it has in its database. For a device with dual Routing Engines, NSM collects the inventory data from the master Routing Engine.

To view the device inventory, the device must be in the Managed state.

**Action**
To view the device inventory, follow these steps:
1. In the navigation tree, select Device Manager > Devices.
2. Right-click the device whose inventory you want to view.
3. Select View/Reconcile Inventory.

The Device Inventory window opens, similar to the example shown in Figure 7 on page 85.
4. Select the **Hardware** tab to display information about hardware modules in the device, including the I/O module, the Routing Engine, and so on. (See Figure 8 on page 85.)

**Figure 8: Viewing the Hardware Inventory**

5. Select the **Software** tab to display information about the software packages installed in the device, including the installed OS and its version, and any other installed packages. (See Figure 9 on page 86.)
NOTE: The License tab not supported for M-series or MX-series devices.

Viewing Device Inventory from the CLI

Purpose The information displayed in the Device Inventory window, as shown in “Viewing Device Inventory in NSM” on page 84 can also be viewed from the device (router) using the CLI operational mode. Generally, the hardware and software information displayed in the Device Inventory window and the CLI command output is similar.

Action To view device hardware and software inventory, from the device enter the following JUNOS CLI operational mode commands:

```plaintext
show chassis hardware
show version
```

Sample Output The following sample output shows hardware and software inventory for the same router used in “Viewing Device Inventory in NSM” on page 84.

```
user@host> show chassis hardware
Hardware inventory:
   Item               Version  Part number  Serial number     Description
   Chassis                                39097             M10i
   Midplane                      REV 04   710-008920   CM0805             M10i Midplane
   Power Supply 0    Rev 06   740-008537   5384103           AC Power Supply
   Power Supply 1    Rev 06   740-008537   5384265           AC Power Supply
   HCM 0            REV 03   710-010580   CM1272            M10i HCM
   HCM 1            REV 03   710-010580   CM1187            M10i HCM
   Routing Engine 0 REV 09   740-009459 1000602468         RE-5.0
   CFEB 0           REV 09   750-010465   DK6820            Internet Processor II
   FPC 0                                                    E-FPC
   PIC 0          REV 10   750-002971   CL0219            4x OC-3 SONET, MM
   PIC 1          REV 11   750-002992   CM4540            4x F/E, 100 BASE-TX
   PIC 2          REV 08   750-005724   CL9082            2x OC-3 ATM-II IQ, MM
   PIC 3          REV 08   750-005724   CL9078            2x OC-3 ATM-II IQ, MM
```
Meaning

The sample output for the `show chassis hardware` command shows the hardware installed on the M10i device. The row of output showing the midplane is in bold to illustrate that the midplane information in this example is identical to the midplane information in the NSM UI example.

The sample output for the `show version` command shows the version of JUNOS software installed on the M10i device. In this instance, the CLI output provides more information than is provided by the NSM UI.

Related Topics

- Managing M-series and MX-series Device Software Versions on page 81
- Viewing and Reconciling Device Inventory on page 83
Chapter 12

Topology Manager

- Overview of the NSM Topology Manager on page 89
- Requisites for a Topology Discovery on page 89
- About the NSM Topology Manager Toolbar on page 90

Overview of the NSM Topology Manager

The Network and Security Manager (NSM) Topology Manager is a tool provided in the NSM user interface (UI) to discover and manage the physical topology of a network of devices connected to a Juniper Networks EX-series switch. These include networking devices such as the J-series, M-series, MX-series, and EX-series, as well as ScreenOS and IDP devices, IP phones, desktops, printers, and servers. The Topology Manager also provides details about connections between a device and the EX-series switch.

For more information about the Topology Manager, see the Network and Security Manager Administration Guide.

Related Topics
- Requisites for a Topology Discovery on page 89
- About the NSM Topology Manager Toolbar on page 90

Requisites for a Topology Discovery

To use the Topology Manager, first add one or more EX-series switches to the Device Manager in NSM. You can then use an added device as a seed device in initiating a topology discovery.

Alternatively, if there are no devices added or managed in NSM, you can initiate a topology discovery by configuring preferred subnets. All the IP addresses in the included subnets range are discovered. Therefore, you need to have either seed devices and/or preferred subnets to initiate topology discovery. You also need:

1. The management IP address of the EX-series switch that acts as the seed IP address
2. SNMP credentials:
   - For SNMPv1 and SNMPv2c: Community string
   - For SNMPv3: Username, security level, authentication type, privacy type, privacy password, and authentication password
3. Enabled Layer 2 protocols like LLDP, STP, RSTP in the switched network, because network discovery depends on these as well as on the Address Forwarding Table information.

For more information about the Topology Manager, see the *Network and Security Manager Administration Guide*.

**Related Topics**
- Overview of the NSM Topology Manager on page 89
- About the NSM Topology Manager Toolbar on page 90

**About the NSM Topology Manager Toolbar**

You can use the Topology Manager toolbar to perform the following actions:

- **Zoom in and Zoom out**: Use these tools to view the network topology according to the detail required. These tools are only of use in the map view.

- **Save to file**: Use this tool to save the network topology map as an image file and the devices and links tables as text files from their respective views.

- **Print**: From different views, you can use this tool to print a network topology map as an image file and the devices and links tables as text files.

- **Manage Devices**: Use this tool to select one or more devices from a topology map and manage them in NSM. This tool is applicable only to map views and not the different table views. To add a device:
  a. Click the *Manage Devices* icon. A dialog box opens.
  b. Enter the SSH user name and password.
  c. Click OK.

- **Set Preferences**: Use this tool to set preferences according to which the discovery engine can perform a topology discovery. You can set preferences for default SNMP credentials, topology discovery intervals, and subnets to be included or excluded.

- **Start and Stop Topology Discovery**: Use these tools to initiate and stop a topology discovery based on the set of seed devices and credentials specified in the topology preferences.

- **Search**: You can search for a device, end-point device, link, or port in any of the table views by providing a string in the search text box. NSM performs a substring match against all attributes of the particular view and displays the results in the same table. If you navigate to another tab, your search results are lost. You can save the search output in a text file as comma-separated values.

The Topology Manager status bar at the bottom of the screen indicates the timestamp of the last completed topology discovery and whether a discovery is in progress.

For more information about the Topology Manager, see the *Network and Security Manager Administration Guide*.

**Related Topics**
- Overview of the NSM Topology Manager on page 89
- Requisites for a Topology Discovery on page 89
Part 5
Monitoring M-series and MX-series Devices

- Real Time Monitoring of M-series and MX-series on page 95
Chapter 13

Real Time Monitoring of M-series and MX-series

- About the Realtime Monitor on page 95
- Viewing Device Status on page 96
- Viewing Device Monitor Alarm Status on page 99
- Setting the Polling Interval For Device Alarm Status on page 100

About the Realtime Monitor

The Realtime Monitor module in Network and Security Manager (NSM) enables you to monitor real-time status and statistics about all the managed devices in your network at a glance. Features of Realtime Monitor enabled for M-series and MX-series include viewing device status, viewing monitor alarm status, and setting the polling interval for device alarm status. You can use the Realtime Monitor to identify problems and discover trends across multiple geographic regions and functional areas from a central management location.

The Realtime Monitor can also help you quickly identify potential device, network, and system-level problems, such as:

- Configuration status—At the device level, you can monitor the changing status of one or more security devices in real time.
- Connection status—At the network level, you can monitor problems that could lead to failed devices.

The Realtime Monitor does the work of a management expert by first gathering information about specific processes and network activity, then color-coding each event to organize problems.

Related Topics

- Viewing Device Status on page 96
- Viewing Device Monitor Alarm Status on page 99
- Setting the Polling Interval For Device Alarm Status on page 100
Viewing Device Status

Table 26 on page 96 lists and describes device information that you can view through the Device Monitor.

Table 26: Device Status Information

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name assigned to the device in NSM.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain in NSM in which the device is managed.</td>
</tr>
<tr>
<td>Platform</td>
<td>Model number of the device.</td>
</tr>
<tr>
<td>OS Version</td>
<td>Operating system firmware version running on the device.</td>
</tr>
</tbody>
</table>
Table 26: Device Status Information (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Status</td>
<td>Current configuration status of the device in NSM:</td>
</tr>
<tr>
<td>None</td>
<td>No state has been set (does not show in Device Monitor).</td>
</tr>
<tr>
<td>Modeled</td>
<td>The device exists in NSM, but a connection to the device has not yet been established.</td>
</tr>
<tr>
<td>RMA</td>
<td>Equivalent to bringing the device into the Modeled state. RMA results from an administrator selection in the UI when a device goes down.</td>
</tr>
<tr>
<td>Waiting for 1st connect</td>
<td>NSM is waiting for the device to connect. You must enter a command on the device to make it connect to NSM.</td>
</tr>
<tr>
<td>Import Needed</td>
<td>You must import the configuration of the device into NSM. When you add a device for the first time, verify that your status indicates “Import Needed” before you attempt to import the device. During migration, this state indicates that import of the security device configuration is still required.</td>
</tr>
<tr>
<td>OS Version Adjustment Needed</td>
<td>The firmware version detected running on the device is different than what was previously detected in NSM. This could happen in the event that the automatic adjustment option was cleared during a change device firmware directive or an Update Device directive was issued to an IDP device with a firmware version mismatch.</td>
</tr>
<tr>
<td>Platform Mismatch</td>
<td>The device platform selected when adding the DMI device in NSM does not match the device itself. A device in this state cannot connect to NSM.</td>
</tr>
<tr>
<td>Device Firmware Mismatch</td>
<td>The OS version selected when adding a DMI device does not match the OS version running on the device itself.</td>
</tr>
<tr>
<td>Device Type Mismatch</td>
<td>The type of device specified when adding the device in NSM does not match the device itself. The device type might indicate whether the device is part of a vsys device, part of a cluster, or part of a virtual chassis. A device in this state cannot connect to NSM.</td>
</tr>
<tr>
<td>Detected duplicate serial number</td>
<td>The device has the same sequence number as another managed device. A device in this state cannot connect to NSM.</td>
</tr>
<tr>
<td>Update Needed</td>
<td>An update to this device is required.</td>
</tr>
<tr>
<td>Managed</td>
<td>The device is currently managed by NSM.</td>
</tr>
<tr>
<td>Managed, In Sync</td>
<td>The physical device configuration is synced with the modeled configuration in NSM.</td>
</tr>
</tbody>
</table>
### Table 26: Device Status Information (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Status (continued)</td>
<td></td>
</tr>
<tr>
<td>Managed, Device Changed—The physical device configuration is out of sync with the modeled configuration in NSM. Changes were made to the physical device configuration (the configuration on the physical device is newer than the modeled configuration). For M-series and MX-series devices with redundant Routing Engines, this status can indicate that a routing engine switchover has occurred.</td>
<td></td>
</tr>
<tr>
<td>Managed, NSM Changed—The modeled device configuration is out of sync with the physical device configuration. Changes were made to the modeled configuration (the configuration on the NSM is newer than the physical device configuration).</td>
<td></td>
</tr>
<tr>
<td>Managed, NSM and Device Changed—Both device configurations (physical and modeled) are out of sync with each other. Changes were made to the physical device configuration and to the modeled configuration.</td>
<td></td>
</tr>
<tr>
<td>Managed, Sync Pending—Completion of the Update Device directive is suspended and waiting for the device to reconnect. This state occurs only for ScreenOS devices that have the Update When Device Connects option selected during the device update.</td>
<td></td>
</tr>
<tr>
<td>Connection Status</td>
<td>Connection status of the device in NSM:</td>
</tr>
<tr>
<td>Up—Device is currently connected to NSM.</td>
<td></td>
</tr>
<tr>
<td>Down—Device is not currently connected to NSM but has connected in the past.</td>
<td></td>
</tr>
<tr>
<td>Never Connected—Device has never connected to NSM.</td>
<td>The Device Server checks the connection status of each device every 120 seconds by default. You can change this behavior by editing the value for the <code>devDaemon.deviceHeartbeatTimeout</code> parameter in the Device Server configuration file. Refer to the <em>Network and Security Manager Installation Guide</em> for more information on editing configuration files.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>If the network connection goes down for a period longer than six to eight minutes, the device connection will permanently time out. If this occurs and the device goes down for any reason, the device still appears as Up in the Device Monitor.</td>
</tr>
<tr>
<td>Alarm</td>
<td>Displays the current alarm status for each device in NSM:</td>
</tr>
<tr>
<td>If device has any alarms, the most severe alarm severity is displayed (either Major or Minor).</td>
<td></td>
</tr>
<tr>
<td>None—The device has no alarms.</td>
<td></td>
</tr>
<tr>
<td>Unknown—The device status is unknown. For example, the device might not be connected.</td>
<td></td>
</tr>
<tr>
<td>N/A—The device’s alarm is not pollable or discoverable, for example, this column shows “N/A” for ScreenOS and IDP devices.</td>
<td></td>
</tr>
<tr>
<td>Alarm is colored:</td>
<td></td>
</tr>
<tr>
<td>Red for Major.</td>
<td></td>
</tr>
<tr>
<td>Orange for Minor.</td>
<td></td>
</tr>
<tr>
<td>Green for Ignore, None, Unknown, or N/A.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 26: Device Status Information (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>H/W Inventory Status</td>
<td>Displays the inventory status for hardware on the device:</td>
</tr>
<tr>
<td></td>
<td>■ In Sync—The inventory information in the NSM database is synchronized with the information on the device.</td>
</tr>
<tr>
<td></td>
<td>■ Out Of Sync—The inventory information in the NSM database is not synchronized with the information on the device.</td>
</tr>
<tr>
<td></td>
<td>■ N/A—The connected device is a ScreenOS or IDP device, or the device is not connected and imported.</td>
</tr>
<tr>
<td>S/W Inventory Status</td>
<td>Displays the inventory status for software on the device:</td>
</tr>
<tr>
<td></td>
<td>■ In Sync—The inventory information in the NSM database is synchronized with the software on the device.</td>
</tr>
<tr>
<td></td>
<td>■ Out Of Sync—The inventory information in the NSM database is not synchronized with the software on the device.</td>
</tr>
<tr>
<td></td>
<td>■ N/A—The connected device is a ScreenOS or IDP device, or the device is not connected and imported.</td>
</tr>
<tr>
<td>License Inventory Status</td>
<td>Displays the inventory status for software on the device:</td>
</tr>
<tr>
<td></td>
<td>■ In Sync—The inventory information in the NSM database is synchronized with the licenses on the device.</td>
</tr>
<tr>
<td></td>
<td>■ Out Of Sync—The inventory information in the NSM database is not synchronized with the licenses on the device.</td>
</tr>
<tr>
<td></td>
<td>■ N/A—The connected device is a ScreenOS or IDP device, or the device is not connected and imported.</td>
</tr>
<tr>
<td>First Connect</td>
<td>The first time the security device connected to the NSM Device Server.</td>
</tr>
<tr>
<td>Latest Connect</td>
<td>The last time the security device connected to the NSM Device Server.</td>
</tr>
<tr>
<td>Latest Disconnect</td>
<td>The last time the security device disconnected from the NSM Device Server.</td>
</tr>
</tbody>
</table>

**Related Topics**
- About the Realtime Monitor on page 95
- Viewing Device Monitor Alarm Status on page 99
- Setting the Polling Interval For Device Alarm Status on page 100

### Viewing Device Monitor Alarm Status

**Purpose**
Alarms refresh automatically through periodic polling.

**Action**
To view the Alarm status and time:

1. From **Device Monitor**, right-click the device row entry and select the **View Alarm** option.

   The device **Alarm Status** dialog box displays the alarm list and polling time for the device.

2. To retrieve the current alarm status in the device, click the **Refresh** button.
The poll time is derived from the device server time.

**Related Topics**
- About the Realtime Monitor on page 95
- Viewing Device Status on page 96
- Setting the Polling Interval For Device Alarm Status on page 100

## Setting the Polling Interval For Device Alarm Status

The default polling interval is 900 seconds (15 minutes). To configure polling intervals for Alarm Status:

1. From **Device Manager > Devices**, double-click the device to open it.

   The Info tab dialog box is displayed.

2. Select the **Device Admin** page to set the polling interval for the device.

   The minimum polling interval is 60 seconds. The maximum interval is 2,147,483,647 seconds. You cannot disable polling.

**Related Topics**
- About the Realtime Monitor on page 95
- Viewing Device Status on page 96
- Viewing Device Monitor Alarm Status on page 99
Part 6
Index

- Index on page 103
Index

A
alarm status
  setting polling intervals...............................100
  viewing................................................................99
API.........................................................................12

C
classifiers
  CoS.......................................................................55
CLI
  about.....................................................................6
  code point aliases...............................................57
  CoS classifiers.......................................................55
  CoS code point aliases.........................................57
  CoS drop profiles..................................................59
  CoS forwarding classes.........................................61
  CoS interfaces......................................................62
  CoS rewrite rules....................................................68
  CoS scheduler maps...............................................72
  CoS schedulers......................................................71
customer support........................................................xviii
  contacting JTAC....................................................xviii

D
data model, defined....................................................10
device
  status.....................................................................16
device configuration
  about.....................................................................41
  modeling..................................................................26
device groups
  planning for..........................................................27
  using.....................................................................27
device inventory
  reconciling............................................................83
  viewing...................................................................83
Device Monitor
  alarm status..........................................................99
  device status information......................................96
device schemas
  about.......................................................................12
devices
  adding multiple with discovery rules......................27
  importing with dynamic IP address........................16
  managed...................................................................23
  modeling..................................................................26
  discovery rules.......................................................27
distributed data collection.........................................12
  DMI See distributed data collection
  drop profiles..........................................................59

Eedit routing-options command................................18

F
forwarding classes.....................................................61

G
group, device...............................................................27

I
inventory See device inventory
  IP addresses
    configuring...........................................................17

J
Job Manager
  about.....................................................................31
  displaying updating errors.....................................35
  reviewing..............................................................33
JUNOS software devices
  adding multiple with discovery rules......................27
  configuring..........................................................42
JUNOS software, upgrading...........................................81

M
M-series devices
  adding multiple with discovery rules......................27
  configuring..........................................................42
  supported Internet routers.....................................15
  managed devices....................................................23
MX-series devices
- adding multiple with discovery rules........27
- configuring........................................42
- supported Internet Services routers........15

N
- navigation tree...........................................6
- NetConf..................................................12
- network
  - connectivity, checking.........................17, 18
  - ping command.......................................17, 18
- no-readvertise
  - option................................................18
- NSM API................................................12
- NSM architecture
  - distributed data collection....................6
- NSM modules
  - Log Viewer..........................................30
  - Realtime Monitor..................................30, 95
- NSM UI
  - about..................................................6
  - navigation tree......................................6

O
- option
  - no-readvertise....................................18
  - retain................................................18

P
- ping command
  - network
    - connectivity, checking......................17, 18

R
- Realtime Monitor
  - using..................................................95
  - retain
    - option...........................................18
  - rewrite rules......................................68
  - role-based administration
    - about............................................4
  - route
    - static...........................................18
  - routers
    - check network connectivity..................17, 18

S
- scheduler maps........................................72
- schedulers............................................71
- schema See device schema
- show route command..............................18

static route..............................................18
status
  - device.............................................16
  - support, technical See technical support

T
- TCP See Transmission Control Protocol
- technical overview.....................................3
- technical support
  - contacting JTAC.....................................xviii
  - Transmission Control Protocol..................12

U
- unreachable workflow
  - importing device...................................16

W
- workflows
  - supported...........................................24