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 the 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 II) 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 présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s’y rattaché, soient redigés 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 ........................................................................................................... xi
- Audience ........................................................................................................... xi
- Conventions ....................................................................................................... xi
- List of Technical Publications ........................................................................... xiii
- Requesting Technical Support ......................................................................... xiii

## Part 1  Getting Started

### Chapter 1  Understanding J-series Services Router and SRX-series Services Gateway Configuration

- NSM and Device Management Overview ............................................................. 3
- Communication Between NSM and a Device Overview ....................................... 3
- Device Configurations Supported in NSM for the J-series Services Router and SRX-series Services Gateway ................................................................. 5

### Chapter 2  J-series Services Routers and SRX-series Services Gateways and NSM Installation and Integration Overview

- J-series Services Router and SRX-series Services Gateway Installation and Configuration Overview ................................................................. 7
- NSM Installation Overview .................................................................................. 8
- Adding J-series Services Routers or SRX-series Services Gateways in NSM Overview ................................................................................................. 8
- Adding J-series Services Router Clusters and SRX-series Services Gateway Clusters Overview ......................................................................................... 8
- Using Templates and Configuration Groups in NSM Overview .......................... 9
Part 2 Configuring J-series Services Routers and SRX-series Services Gateways

Chapter 3 Configuring User Authentication in J-series Services Routers and SRX-series Services Gateways 13

Configuring RADIUS Authentication (NSM Procedure) ........................................... 13
Configuring TACACS+ Authentication (NSM Procedure) ........................................ 14
Configuring Authentication Order (NSM Procedure) .............................................. 15
Configuring User Access (NSM Procedure) ......................................................... 16
  Configuring Login Classes .................................................................................. 16
  Configuring User Accounts .............................................................................. 17
Configuring Template Accounts (NSM Procedure) ................................................ 17
  Creating a Remote Template Account ................................................................. 18
  Creating a Local Template Account .................................................................. 19

Chapter 4 Configuring USB Modem Interfaces in J-series Services Routers and SRX-series Services Gateways 21

Configuring a USB Modem Interface (NSM Procedure) ............................................ 21
Configuring a Dialer Interface (NSM Procedure) .................................................... 22
Configuring Dial-in Options on a Dialer Interface (NSM Procedure) ...................... 23
Configuring a CHAP Access Profile on a Dialer Interface (NSM Procedure) ....... 24

Chapter 5 Configuring SNMP for Network Management in J-series Services Routers and SRX-series Services Gateways 27

Configuring Basic System Identification for SNMP (NSM Procedure) ..................... 27
Configuring SNMP Agents and Communities (NSM Procedure) ......................... 28
Configuring SNMP Trap Groups (NSM Procedure) .............................................. 29
Configuring SNMP Views (NSM Procedure) ....................................................... 30

Chapter 6 Configuring J-series Services Routers and SRX-series Services Gateways for DHCP 33

Configuring the Device as a DHCP Server (NSM Procedure) .................................. 33
Configuring the Device as a DHCP Client (NSM Procedure) .................................. 35

Chapter 7 Configuring Class of Service in J-series Services Routers and SRX-series Services Gateways 37

Configuring CoS Classifiers (NSM Procedure) ...................................................... 37
Configuring CoS Code Point Aliases (NSM Procedure) ........................................ 39
Configuring CoS Drop Profile (NSM Procedure) ................................................... 41
Configuring CoS Forwarding Classes (NSM Procedure) ....................................... 43
Configuring CoS Interfaces (NSM Procedure) ...................................................... 44
Part 3
Managing J-series Services Routers and SRX-series Services Gateways

Chapter 8
Using System Management Features in J-series Services Routers and SRX-series Services Gateways

Managing J-series and SRX-series Device Software Versions Overview ..........59
Viewing and Reconciling Device Inventory Overview ..................................59
Viewing Device Inventory in NSM (NSM Procedure) ..................................60
Removing a J-series or SRX-series Device from NSM Management (NSM Procedure) .................................................................61

Chapter 9
Topology Manager

Overview of the NSM Topology Manager ..................................................63
Requisites for a Topology Discovery Overview .........................................63
Understanding the NSM Topology Manager Toolbar ...............................64

Part 4
Monitoring J-series Services Routers and SRX-series Services Gateways

Chapter 10
Real Time Monitoring of J-series Services Routers and SRX-series Services Gateways

Realtime Monitor Overview ........................................................................69
Viewing Device Status .............................................................................70
Viewing Device Monitor Alarm Status (NSM Procedure) ...........................72
Configuring the Polling Interval for Device Alarm Status (NSM Procedure) .........................................................................................73

Part 5
Index

Index ............................................................................................................77
About this Guide

Objectives

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 security devices.

This guide provides the information you need to understand, configure, and maintain J-series Services Routers and SRX-series Services Gateways using NSM. The J-series and SRX-series device configuration features that are detailed in this guide are as follows:

- User Authentication
- USB Modem Interfaces
- SNMP
- DHCP
- Class of Service

For details on configuring specific J-series and SRX-series features, see their respective JUNOS configuration guides.

Audience

This guide is for the system administrator responsible for configuring J-series Services Routers and SRX-series Services Gateways.

Conventions

Table 1 on page xii defines notice icons used in this guide.
Table 1: Notice Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Note Icon]</td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td>![Caution Icon]</td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td>![Warning Icon]</td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td>![Laser Warning Icon]</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 xii defines text conventions used in this guide.

Table 2: Text Conventions

<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.</td>
<td>Issue the <code>clock source</code> command. Specify the keyword <code>exp-msg</code>. Click User Objects</td>
</tr>
<tr>
<td></td>
<td>Represents keywords</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Represents UI elements</td>
<td></td>
</tr>
<tr>
<td>Fixed-width font</td>
<td>Represents information as displayed on the terminal screen.</td>
<td><code>host1# show ip ospf Routing Process OSPF 2 with Router ID 5.5.0.250</code> 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><code>Ctrl + d</code></td>
</tr>
<tr>
<td>Italics</td>
<td>Emphasizes words</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identifies variables</td>
<td></td>
</tr>
<tr>
<td>The angle bracket (&gt;)</td>
<td>Indicates navigation paths through the UI by clicking menu options and links.</td>
<td><code>Object Manager &gt; User Objects &gt; Local Objects</code></td>
</tr>
</tbody>
</table>

Table 3 on page xiii 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 ( [ ] )</td>
<td>Represent optional keywords or variables.</td>
<td>[ internal</td>
</tr>
<tr>
<td>Words enclosed in brackets followed by and asterisk ( [ ]* )</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 ( { } )</td>
<td>Represent required keywords or variables.</td>
<td>{ permit</td>
</tr>
</tbody>
</table>

### List of Technical Publications

#### Table 4: Network and Security Manager Publications

<table>
<thead>
<tr>
<th>Publication</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network and Security Manager Installation Guide</td>
<td>Details 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 and/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 where applicable. 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 Firewall/VPN Devices Guide</td>
<td>Describes NSM features that relate to device configuration and management. It also explains how to configure basic and advanced NSM functionality, including deploying new device configurations, managing Security Policies and VFPNs, and general device administration.</td>
</tr>
<tr>
<td>Network and Security Manager Online Help</td>
<td>Provides task-oriented procedures describing how to perform 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>
</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/](http://www.juniper.net/customers/support/)

- **Search for known bugs**: [http://www2.juniper.net/kb/](http://www2.juniper.net/kb/)

- **Find product documentation**: [http://www.juniper.net/techpubs/](http://www.juniper.net/techpubs/)

- **Find solutions and answer questions using our Knowledge Base**: [http://kb.juniper.net/](http://kb.juniper.net/)

- **Download the latest versions of software and review release notes**: [http://www.juniper.net/customers/csc/software/](http://www.juniper.net/customers/csc/software/)

- **Search technical bulletins for relevant hardware and software notifications**: [https://www.juniper.net/alerts/](https://www.juniper.net/alerts/)

- **Join and participate in the Juniper Networks Community Forum**: [http://www.juniper.net/company/communities/](http://www.juniper.net/company/communities/)

- **Open a case online in the CSC Case Management tool**: [http://www.juniper.net/cm/](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/](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/](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](http://www.juniper.net/support/requesting support.html)
Part 1
Getting Started

- Understanding J-series Services Router and SRX-series Services Gateway Configuration on page 3
- J-series Services Routers and SRX-series Services Gateways and NSM Installation and Integration Overview on page 7
Chapter 1
Understanding J-series Services Router and SRX-series Services Gateway
Configuration

- NSM and Device Management Overview on page 3
- Communication Between NSM and a Device Overview on page 3
- Device Configurations Supported in NSM for the J-series Services Router and SRX-series Services Gateway on page 5

NSM and Device Management Overview

NSM is the Juniper Networks network management tool that allows distributed administration of network appliances. You can use the NSM application to centralize status monitoring, logging, and reporting, and to administer device configurations. 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 device’s admin console. The configuration screens rendered through NSM are similar to the screens in the device’s admin console.

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
- Communication Between NSM and a Device Overview on page 3
- Device Configurations Supported in NSM for the J-series Services Router and SRX-series Services Gateway on page 5

Communication Between NSM and a Device Overview

The NSM application and a device communicate through the Device Management Interface (DMI). DMI is a collection of schema-driven protocols that run on a common transport (that is, TCP). DMI is designed to work with Juniper Networks platforms to
make device management consistent across all administrative realms. Supported DMI protocols include:

- NetConf (for inventory management, XML-based configuration, text-based configuration, alarm monitoring, and device specific commands)
- Structured syslog
- 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 device’s configuration is represented as a hierarchical tree of configuration items. This structure is expressed in XML and can be manipulated with NetConf. NetConf is a network management protocol that uses XML. DMI uses NetConf’s generic configuration management capability to allow remote configuration of the device.

To allow NSM to manage the device using the DMI protocol, NSM must import the schema and metadata files from the Juniper Networks Schema Repository, a publicly accessible resource that is updated with each device release. In addition to downloading the device’s current schema, NSM may also download upgraded software.

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

Before attempting to communicate with NSM, you must first complete the initial configuration of the device. Initial configuration includes network interface settings, DNS settings, licensing, and password administration.

If you have several devices that will be configured in a clustering environment, the cluster abstraction must first be created in the NSM Cluster Manager. Then you can add individual nodes.

After you have completed the initial network configuration, you can configure the device to communicate with NSM using the appropriate network information. Once the device has been configured to communicate with NSM, the device contacts NSM and establishes a DMI session through an initial TCP handshake.

All communications between the device and NSM occur over SSH to ensure data integrity.

After the device initially contacts NSM and a TCP session is established, interaction between the device and NSM is driven from NSM, which issues commands to get hardware, software, and license details of the device. NSM connects to the Schema Repository to download the configuration schema that is specific to the device.

NSM then issues a command to retrieve configuration information from the device. If NSM is contacted by more than one device as a member of a cluster, information from only one of the cluster devices is gathered. NSM attempts to validate the configuration received from the device against the schema from Juniper Networks.

Once the device and NSM are communicating, the device delivers syslog and event information to NSM.
After NSM and the device are connected, you can make any configuration changes directly on the device, bypassing NSM. NSM automatically detects these changes and imports the new configuration data. Changes to device cluster members will similarly be detected by NSM.

When you make changes to the device’s configuration through NSM, you must push the changes to the device by performing an Update Device operation.

When you double-click the device icon in the Device Manager and select the **Configuration** tab, the configuration tree appears in the main display area in the same orientation as items appear on the device’s admin console.

**Related Topics**

- NSM and Device Management Overview on page 3
- Device Configurations Supported in NSM for the J-series Services Router and SRX-series Services Gateway on page 5

## Device Configurations Supported in NSM for the J-series Services Router and SRX-series Services Gateway

J-series Services Router and SRX-series services gateway support the following services in NSM:

- **Inventory management service**—Enables management of the software, hardware, and licensing details for the J-series Services Router and the SRX-series services gateway. Adding or deleting licenses and upgrading or downgrading software are not supported.

- **Status monitoring service**—Allows the status of the J-series Services Router and the SRX-series services gateway to be obtained, including name, domain, OS version, synchronization status, connection details, and current alarms.

- **Logging service**—Allows logs to be obtained in a time-generated order for the J-series Services Router and the SRX-series services gateway device. Logging configuration details that are set on the J-series Services Router and the SRX-series services gateway will apply to NSM.

- **XML-based configuration management service**—Enables NSM to manage the configuration of the J-series Services Router and the SRX-series services gateway. NSM uses the same XML schema as the J-series Services Router and the SRX-series services gateway, so you can troubleshoot NSM using XML files downloaded from either device.

The following device configurations are not supported:

- Editing licensing information, although licenses can be viewed
- Packaging log files or debug files for remote analysis
- Rebooting the J-series Services Router and SRX-series services gateway

**Related Topics**

- NSM and Device Management Overview on page 3
- Communication Between NSM and a Device Overview on page 3
Chapter 2

J-series Services Routers and SRX-series Services Gateways and NSM Installation and Integration Overview

- J-series Services Router and SRX-series Services Gateway Installation and Configuration Overview on page 7
- NSM Installation Overview on page 8
- Adding J-series Services Routers or SRX-series Services Gateways in NSM Overview on page 8
- Adding J-series Services Router Clusters and SRX-series Services Gateway Clusters Overview on page 8
- Using Templates and Configuration Groups in NSM Overview on page 9

J-series Services Router and SRX-series Services Gateway Installation and Configuration Overview

**NOTE:** For important safety information, read the *Juniper Networks Security Products Safety Guide.*

Before you can add either a J-series Services Router or an SRX-series services gateway to NSM, the device must be installed and configured, and logon credentials for an NSM administrator must be configured for it. Follow these steps:

1. Connect the device to the network and configure one of the interfaces so that the device can reach the NSM device server.
2. Add a user for NSM that has full administrative rights.

For complete details on installing and configuring J-series Services Routers, see the corresponding Hardware Guide for your device.

For complete details on installing and configuring SRX-series services gateway, see the corresponding Hardware Guide for your device.

**Related Topics**

- NSM Installation Overview on page 8
- NSM and Device Management Overview on page 3
NSM Installation Overview

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).

See the Network Security Manager Installation Guide for 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 installing or upgrading NSM.

Related Topics
- J-series Services Router and SRX-series Services Gateway Installation and Configuration Overview on page 7
- NSM and Device Management Overview on page 3

Adding J-series Services Routers or SRX-series Services Gateways in NSM Overview

Before NSM can manage devices, you must first add those devices to the management system using the NSM 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.

For complete details on adding J-series Services Routers or SRX-series services gateways, see the Network and Security Manager Administration Guide.

Related Topics
- NSM and Device Management Overview on page 3
- Communication Between NSM and a Device Overview on page 3
- Device Configurations Supported in NSM for the J-series Services Router and SRX-series Services Gateway on page 5
- Adding J-series Services Router Clusters and SRX-series Services Gateway Clusters Overview on page 8

Adding J-series Services Router Clusters and SRX-series Services Gateway Clusters Overview

A cluster consists of multiple devices joined together in a high availability configuration to ensure continued network uptime. The device configurations are synchronized, meaning all cluster members share the same configuration settings, enabling a device to handle traffic for another if one device fails.
Adding a cluster is a two-stage process:
- Add the cluster device object.
- Add the members of the cluster to the cluster device object.

For complete details on adding J-series Services Router clusters or SRX-series services gateway clusters, see the Network and Security Manager Administration Guide.

Related Topics
- NSM and Device Management Overview on page 3
- Communication Between NSM and a Device Overview on page 3
- Device Configurations Supported in NSM for the J-series Services Router and SRX-series Services Gateway on page 5
- Adding J-series Services Routers or SRX-series Services Gateways in NSM Overview on page 8

Using Templates and Configuration Groups in NSM Overview

Use templates to define a common device configuration and then reuse that configuration information across multiple devices. In a template, you need to define only those configuration parameters that you want to set; you do not need to specify a complete device configuration.

Templates provide these benefits:
- You can configure parameter values for a device by referring to one or more templates when configuring the device.
- When you change a parameter value in a template and save the template, the value also changes for all device configurations that refer to that template, unless specifically overridden in the device object.

For complete details on using device templates and configuration groups, see the Network and Security Manager Administration Guide.

Related Topics
- Adding J-series Services Routers or SRX-series Services Gateways in NSM Overview on page 8
- Adding J-series Services Router Clusters and SRX-series Services Gateway Clusters Overview on page 8
Part 2
Configuring J-series Services Routers and SRX-series Services Gateways

- Configuring User Authentication in J-series Services Routers and SRX-series Services Gateways on page 13
- Configuring USB Modem Interfaces in J-series Services Routers and SRX-series Services Gateways on page 21
- Configuring SNMP for Network Management in J-series Services Routers and SRX-series Services Gateways on page 27
- Configuring J-series Services Routers and SRX-series Services Gateways for DHCP on page 33
- Configuring Class of Service in J-series Services Routers and SRX-series Services Gateways on page 37
Chapter 3
Configuring User Authentication in J-series Services Routers and SRX-series Services Gateways

- Configuring RADIUS Authentication (NSM Procedure) on page 13
- Configuring TACACS+ Authentication (NSM Procedure) on page 14
- Configuring Authentication Order (NSM Procedure) on page 15
- Configuring User Access (NSM Procedure) on page 16
- Configuring Template Accounts (NSM Procedure) on page 17

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 5 on page 14.
5. Click one:
   ■ New—Adds a new RADIUS server.
   ■ OK—Saves the changes.
   ■ Cancel—Cancels the modifications.
Table 5: 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>
<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 14
- Configuring Authentication Order (NSM Procedure) on page 15
- Configuring User Access (NSM Procedure) on page 16

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 6 on page 14.
5. Click one:
   - New—Adds a new TACACS+ server.
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Table 6: 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>
</tbody>
</table>
Table 6: TACACS+ Authentication Configuration Details (continued)

<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 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>
<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 13
- Configuring Authentication Order (NSM Procedure) on page 15
- Configuring User Access (NSM Procedure) on page 16

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 13
- Configuring TACACS+ Authentication (NSM Procedure) on page 14
- Configuring User Access (NSM Procedure) on page 16
Configuring User Access (NSM Procedure)

This section includes the following topics:

- Configuring Login Classes on page 16
- Configuring User Accounts on page 17

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 7 on page 16.
5. Click one:
   - New—Adds a new login class.
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

<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 8 on page 17.
5. Click one:
   - **New**—Adds a new user account.
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

### Table 8: 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>

<table>
<thead>
<tr>
<th>Login &gt; User &gt; Authentication</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain Text Password Value</td>
<td>Specifies the user’s password.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring RADIUS Authentication (NSM Procedure) on page 13
- Configuring TACACS+ Authentication (NSM Procedure) on page 14
- Configuring Authentication Order (NSM Procedure) on page 15

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 18
■ Creating a Local Template Account on page 19

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 9 on page 18.
5. Click one:
   ■ New—Creates a new remote template account.
   ■ OK—Saves the changes.
   ■ Cancel—Cancels the modifications.

Table 9: 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 10 on page 19.
5. Click one:
   - New—Creates a new local template account.
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

<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 admin.</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 superuser</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring RADIUS Authentication (NSM Procedure) on page 13
- Configuring TACACS+ Authentication (NSM Procedure) on page 14
- Configuring Authentication Order (NSM Procedure) on page 15
Chapter 4

Configuring USB Modem Interfaces in J-series Services Routers and SRX-series Services Gateways

- Configuring a USB Modem Interface (NSM Procedure) on page 21
- Configuring a Dialer Interface (NSM Procedure) on page 22
- Configuring Dial-in Options on a Dialer Interface (NSM Procedure) on page 23
- Configuring a CHAP Access Profile on a Dialer Interface (NSM Procedure) on page 24

Configuring a USB Modem Interface (NSM Procedure)

To configure a USB modem interface for the device:

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 the USB modem interface.
3. Click the Configuration tab. In the configuration tree, select Interfaces > Interfaces List.
4. Add or modify interface settings as specified in Table 11 on page 21.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 11: USB Modem Interface 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 name of the new interface.</td>
<td>Enter a name for the new interface.</td>
</tr>
</tbody>
</table>

Dialer Options > Pool
Table 11: USB Modem Interface Configuration Details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the dialer pool configured on the dialer interface you want to use for USB modem connectivity.</td>
<td>Enter a name for the dialer pool.</td>
</tr>
<tr>
<td>Priority</td>
<td>Specifies the dialer pool priority.</td>
<td>Set the dialer pool priority.</td>
</tr>
</tbody>
</table>

**Modem Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Init Command String</td>
<td>Configures the modem to automatically answer calls after a specified number of rings.</td>
<td>Enter the modem initialization command string. For example, enter ATSO = 2.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring a Dialer Interface (NSM Procedure) on page 22
- Configuring Dial-in Options on a Dialer Interface (NSM Procedure) on page 23

### Configuring a Dialer Interface (NSM Procedure)

To configure a dialer interface for the device:

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 the dialer interface.
3. Click the **Configuration** tab. In the configuration tree, select **Interfaces > Interfaces List**.
4. Add or modify interface settings as specified in Table 12 on page 22.
5. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 12: Dialer Interface 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 name of the new interface.</td>
<td>Enter a name for the new interface.</td>
</tr>
<tr>
<td>Description</td>
<td>Differentiates between different dialer interfaces.</td>
<td>Enter a description for the new interface.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Specifies the encapsulation.</td>
<td>Select <strong>PPP</strong> from the encapsulation list.</td>
</tr>
</tbody>
</table>
Table 12: Dialer Interface Configuration Details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unit</td>
<td>Specifies the logical unit.</td>
<td>Enter the unit number.</td>
</tr>
<tr>
<td>Unit &gt; Dialer Options</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pool</td>
<td>Specifies the name of the dialer pool to use for USB modem connectivity.</td>
<td>Enter the name of the dialer pool.</td>
</tr>
<tr>
<td>Unit &gt; Family &gt; Inet &gt; Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the source IP address for the dialer interface.</td>
<td>Enter the source IP address.</td>
</tr>
<tr>
<td>Destination</td>
<td>Specifies the destination IP address for the dialer interface.</td>
<td>Enter the destination IP address.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring a USB Modem Interface (NSM Procedure) on page 21
- Configuring Dial-in Options on a Dialer Interface (NSM Procedure) on page 23

Configuring Dial-in Options on a Dialer Interface (NSM Procedure)

To configure dial-in options on a dialer interface:

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 dial-in options.
3. Click the Configuration tab. In the configuration tree, select Interfaces > Interfaces List.
4. Select the dialer interface and add or modify interface settings as specified in Table 13 on page 23.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 13: Dialer Interface for Dial-in Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit &gt; Dialer Options &gt; Incoming Map</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Caller</td>
<td>Specifies the incoming map options for the dialer interface.</td>
<td>Select accept-all to accept all incoming calls. Select caller to accept calls from a specific caller ID.</td>
</tr>
</tbody>
</table>
Table 13: Dialer Interface for Dial-in Configuration Details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caller</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the caller ID to be accepted on the dialer interface.</td>
<td>Enter the caller ID.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring a Dialer Interface (NSM Procedure) on page 22
- Configuring a USB Modem Interface (NSM Procedure) on page 21

**Configuring a CHAP Access Profile on a Dialer Interface (NSM Procedure)**

To configure a CHAP access profile on a dialer interface:

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 CHAP.
3. Click the **Configuration** tab. In the configuration tree, select **Access > Profile** to define a CHAP access profile.
4. Add or modify CHAP access settings as specified in Table 14 on page 24.
5. Click the **Configuration** tab. In the configuration tree, select **Interfaces > Interfaces List** to configure CHAP on the dialer interface.
6. Select the appropriate dialer interface level, and add or modify interface settings as specified in Table 15 on page 25.
7. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 14: CHAP Access Profile 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 profile.</td>
<td>Enter a name for the profile.</td>
</tr>
<tr>
<td>Client</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies a name for the client.</td>
<td>Enter a name for the client.</td>
</tr>
<tr>
<td>Chap Secret</td>
<td>Specifies the CHAP secret.</td>
<td>Enter the CHAP secret.</td>
</tr>
</tbody>
</table>

**NOTE:** Enter the client name and CHAP secret for each client to be included in the CHAP profile.
### Table 15: CHAP Dialer Interface Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unit</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unit</td>
<td>Specifies the logical unit.</td>
<td>Enter the unit number.</td>
</tr>
<tr>
<td><strong>Unit &gt; Ppp Options &gt; Chap</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access profile</td>
<td>Specifies the profile name.</td>
<td>Enter a unique profile name containing a client list and access parameters.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring a Dialer Interface (NSM Procedure) on page 22
- Configuring a USB Modem Interface (NSM Procedure) on page 21
Chapter 5
Configuring SNMP for Network Management in J-series Services Routers and SRX-series Services Gateways

- Configuring Basic System Identification for SNMP (NSM Procedure) on page 27
- Configuring SNMP Agents and Communities (NSM Procedure) on page 28
- Configuring SNMP Trap Groups (NSM Procedure) on page 29
- Configuring SNMP Views (NSM Procedure) on page 30

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 16 on page 27.
5. Click one:
   - OK—Saves the changes.
   - Cancel—Cancels the modifications.

Table 16: 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>
</tbody>
</table>
### Table 16: Basic System Identification Details (continued)

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

**Related Topics**
- Configuring SNMP Agents and Communities (NSM Procedure) on page 28
- Configuring SNMP Trap Groups (NSM Procedure) on page 29
- Configuring SNMP Views (NSM Procedure) on page 30

### 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 17 on page 28.
5. Click one:
   - **New**—Creates a new community.
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

### Table 17: 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>

---

28 — Configuring SNMP Agents and Communities (NSM Procedure)
Table 17: 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>Name</td>
<td>Specifies community access to a client at a particular IP address.</td>
<td>Enter the IP address.</td>
</tr>
<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 27
- Configuring SNMP Trap Groups (NSM Procedure) on page 29
- Configuring SNMP Views (NSM Procedure) on page 30

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 18 on page 29.
5. Click one:
   - **New**—Creates a new SNMP trap group.
   - **OK**—Saves the changes.
   - **Cancel**— Cancels the modifications.

Table 18: 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
Table 18: SNMP Trap Group Configuration Details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Define the types of traps that will be sent to the targets of the named trap group.</td>
<td>Select the trap type.</td>
</tr>
</tbody>
</table>

**Snmp > Trap Group > Targets**

| Name                 | Specifies the IPv4 or IPv6 address of the system to receive traps. | Enter the IPv4 or IPv6 address of the system, but not a hostname. |

Related Topics
- Configuring Basic System Identification for SNMP (NSM Procedure) on page 27
- Configuring SNMP Agents and Communities (NSM Procedure) on page 28
- Configuring SNMP Views (NSM Procedure) on page 30

**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 19 on page 30.
5. Click one:
   - **New**—Creates a new view.
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

Table 19: 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>
</tbody>
</table>

**Snmp > View > Oid**

| Name | Specifies the MIB for the view. | Enter the OID of the MIB in either dotted integer or subtree name format. |

Include or Exclude | Specifies whether the view includes or excludes the MIB | Select this option. |

Related Topics
- Configuring Basic System Identification for SNMP (NSM Procedure) on page 27
Chapter 5: Configuring SNMP for Network Management in J-series Services Routers and SRX-series Services Gateways

- Configuring SNMP Agents and Communities (NSM Procedure) on page 28
- Configuring SNMP Trap Groups (NSM Procedure) on page 29
Chapter 6

Configuring J-series Services Routers and SRX-series Services Gateways for DHCP

- Configuring the Device as a DHCP Server (NSM Procedure) on page 33
- Configuring the Device as a DHCP Client (NSM Procedure) on page 35

Configuring the Device as a DHCP Server (NSM Procedure)

The Dynamic Host Configuration Protocol (DHCP) server provides a framework for passing configuration information to client hosts (such as PCs) on a TCP/IP network. A router or interface that acts as a DHCP server can allocate network IP addresses and deliver configuration settings to client hosts without user intervention. DHCP access service minimizes the overhead required to add clients to the network by providing a centralized, server-based setup. You do not have to manually create and maintain IP address assignments for clients.

To configure the device as a DHCP server for a subnet and a single client:

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 DHCP server.
3. Click the Configuration tab. In the configuration tree, select System > Services > Dhcp.
4. Add or modify DHCP settings as specified in Table 20 on page 33.
5. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Table 20: DHCP Server Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Lease Time</td>
<td>Specifies the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server.</td>
<td>Select the maximum lease time.</td>
</tr>
</tbody>
</table>
Table 20: DHCP Server Configuration Details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Lease Time</td>
<td>Specifies the length of time in seconds that a client holds the lease for an IP address assigned by a DHCP server. This setting is used if a lease time is not requested by the client.</td>
<td>Select the default lease time.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Specifies the name of the domain in which clients search for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified.</td>
<td>Enter the domain name.</td>
</tr>
<tr>
<td>Boot File</td>
<td>Specifies the boot file advertised to DHCP clients. After the client receives an IP address and the boot file location from the DHCP server, the client uses the boot image stored in the boot file to complete DHCP setup.</td>
<td>Enter the location of the boot file on the boot server. The filename can include a path name.</td>
</tr>
<tr>
<td>Boot Server</td>
<td>Specifies the name of the boot server advertised to DHCP clients. The client uses a boot file located on the boot server to complete DHCP setup.</td>
<td>Enter the address of a boot server. You must specify an IPv4 address, not a hostname.</td>
</tr>
<tr>
<td>Server Identifier</td>
<td>Specifies the server identifier. This is an optional setting that can be used to identify a DHCP server in a DHCP message.</td>
<td>Enter the IPv4 address of the server. This address must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding).</td>
</tr>
</tbody>
</table>

**Dhcp > Pool**

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the logical subnet address or netmask.</td>
<td>Enter the IP address pool range.</td>
</tr>
<tr>
<td>Low</td>
<td>Specifies lowest IP address in the pool that is available for dynamic address assignment.</td>
<td>Enter the IP address.</td>
</tr>
<tr>
<td>High</td>
<td>Specifies highest IP address in the pool that is available for dynamic address assignment.</td>
<td>Enter the IP address.</td>
</tr>
</tbody>
</table>

**Dhcp > Domain Search**

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the domain search suffixes to be used by the clients.</td>
<td>Enter the list of domain names to search. The list can contain up to 6 domain names, with a total of up to 256 characters.</td>
</tr>
</tbody>
</table>
### Table 20: DHCP Server Configuration Details (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dhcp &gt; Name Server</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Defines a Domain Name System (DNS) name server.</td>
<td>Enter the address of the name server. To configure multiple name servers, include multiple address options.</td>
</tr>
<tr>
<td><strong>Dhcp &gt; Option</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the ID number that indexes the option and must be unique across a DHCP server.</td>
<td>Select the ID number.</td>
</tr>
<tr>
<td>Flag</td>
<td>Specifies the option type.</td>
<td>Select the option type.</td>
</tr>
<tr>
<td><strong>Dhcp &gt; Static Binding</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the MAC address of the client. This is a hardware address that uniquely identifies a client on the network.</td>
<td>Enter the MAC address of the client.</td>
</tr>
<tr>
<td><strong>Dhcp &gt; Static Binding &gt; Fixed Address</strong></td>
<td>Specifies the fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.</td>
<td>Enter the fixed IP address.</td>
</tr>
</tbody>
</table>

### Related Topics
- Configuring the Device as a DHCP Client (NSM Procedure) on page 35

### Configuring the Device as a DHCP Client (NSM Procedure)

A device can act as a DHCP client, receiving its TCP/IP settings and the IP address for any physical interface in any security zone from an external DHCP server. The device can also act as a DHCP server, providing TCP/IP settings and IP addresses to clients in any zone.

To configure the device as a DHCP client:

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 DHCP client.
3. Click the Configuration tab. In the configuration tree, select Interfaces.
4. Select the interface on which you want to configure DHCP client information, and select Unit > Family > Inet > Dhcp.
5. Click **Enable** next to Dhcp, and add or modify DHCP settings as specified in Table 21 on page 36.

6. Click one:
   - **OK**—Saves the changes.
   - **Cancel**—Cancels the modifications.

### Table 21: DHCP Client Configuration Details

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lease Time</td>
<td>Specifies the DHCP lease time in seconds.</td>
<td>Enter the DHCP lease time in seconds.</td>
</tr>
<tr>
<td>Retransmission Attempt</td>
<td>Specifies the number of attempts allowed to retransmit a DHCP packet.</td>
<td>Enter the number of attempts allowed to retransmit a DHCP packet.</td>
</tr>
<tr>
<td>Retransmission Interval</td>
<td>Specifies the interval allowed between retransmission attempts in seconds.</td>
<td>Enter the interval allowed between retransmission attempts in seconds.</td>
</tr>
<tr>
<td>Server Address</td>
<td>Specifies the IPv4 address of the preferred DHCP server.</td>
<td>Enter the IPv4 address of the preferred DHCP server.</td>
</tr>
<tr>
<td>Vendor Id</td>
<td>Specifies the vendor class ID for the DHCP client.</td>
<td>Enter the vendor class ID.</td>
</tr>
</tbody>
</table>

**Dhcp > Client Identifier**

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ascii</td>
<td>Specifies the DHCP client identifier as either an ASCII or hexadecimal value.</td>
<td>Select the DHCP client identifier, and type the ASCII or hexadecimal value.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring the Device as a DHCP Server (NSM Procedure) on page 33
Chapter 7

Configuring Class of Service in J-series Services Routers and SRX-series Services Gateways

- Configuring CoS Classifiers (NSM Procedure) on page 37
- Configuring CoS Code Point Aliases (NSM Procedure) on page 39
- Configuring CoS Drop Profile (NSM Procedure) on page 41
- Configuring CoS Forwarding Classes (NSM Procedure) on page 43
- Configuring CoS Interfaces (NSM Procedure) on page 44
- Configuring CoS Rewrite Rules (NSM Procedure) on page 49
- Configuring CoS Schedulers (NSM Procedure) on page 52
- Configuring CoS and Applying Scheduler Maps on page 54

Configuring CoS Classifiers (NSM Procedure)

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 22 on page 38.

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 22: 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-of-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 22: Configuring and Applying Behavior Aggregate Classifiers (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure an assured 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 assured forwarding—for example, class-af-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 assured forwarding traffic—for example, 001100.</td>
</tr>
<tr>
<td></td>
<td>7. Click OK three times.</td>
</tr>
<tr>
<td>Apply the behavior aggregate classifier to an interface.</td>
<td>1. Click Add new entry next to Interfaces.</td>
</tr>
<tr>
<td></td>
<td>2. In the Interface name box, type the name of the interface—for example, ge-0/0/0.</td>
</tr>
<tr>
<td></td>
<td>3. Click Add new entry next to Unit.</td>
</tr>
<tr>
<td></td>
<td>4. In the Unit number box, type the logical interface unit number—for example, 0.</td>
</tr>
<tr>
<td></td>
<td>5. Click Configure next to Classifiers.</td>
</tr>
<tr>
<td></td>
<td>6. In the Classifiers box, under Dscp, type the name of the previously configured behavior aggregate classifier—for example, ba-classifier.</td>
</tr>
<tr>
<td></td>
<td>7. Click OK.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring CoS Code Point Aliases (NSM Procedure) on page 39
- Configuring CoS Drop Profile (NSM Procedure) on page 41
- Configuring CoS Forwarding Classes (NSM Procedure) on page 43
- Configuring CoS Interfaces (NSM Procedure) on page 44
- Configuring CoS Rewrite Rules (NSM Procedure) on page 49
- Configuring CoS Schedulers (NSM Procedure) on page 52
- Configuring CoS and Applying Scheduler Maps on page 54

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 23 on page 40.
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 23: Configuring Code Point Aliases

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

**Related Topics**
- Configuring CoS Classifiers (NSM Procedure) on page 37
- Configuring CoS Drop Profile (NSM Procedure) on page 41
- Configuring CoS Forwarding Classes (NSM Procedure) on page 43
- Configuring CoS Interfaces (NSM Procedure) on page 44
- Configuring CoS Rewrite Rules (NSM Procedure) on page 49
- Configuring CoS Schedulers (NSM Procedure) on page 52
- Configuring CoS and Applying Scheduler Maps on page 54
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 24 on page 41.
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 24: Drop Profile Configuration Fields

<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>
| Name         | Specifies the drop profile name. | 1. Click the New button or Edit button in the Drop Profile interface.  
|              |                           | 2. Enter the drop profile name in the Name box.                             |
Table 24: Drop Profile Configuration Fields *(continued)*

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</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>
<tr>
<td>Fill Level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</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>Comment</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 37
- Configuring CoS Code Point Aliases (NSM Procedure) on page 39
- Configuring CoS Forwarding Classes (NSM Procedure) on page 43
- Configuring CoS Interfaces (NSM Procedure) on page 44
- Configuring CoS Rewrite Rules (NSM Procedure) on page 49
- Configuring CoS Schedulers (NSM Procedure) on page 52
- Configuring CoS and Applying Scheduler Maps on page 54
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 25 on page 43.
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 25: Assigning Forwarding Classes to Output Queues

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign best-effort traffic to queue 0.</td>
<td>1. Select Queue and click <strong>Add new entry</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the Queue num box, type 0.</td>
</tr>
<tr>
<td></td>
<td>3. In the Class name box, type the previously configured name of the best-effort class—for example, <strong>be-class</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong></td>
</tr>
<tr>
<td>Assign expedited forwarding traffic to queue 1.</td>
<td>1. Select Queue and click <strong>Add new entry</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the Queue num box, type 1.</td>
</tr>
<tr>
<td></td>
<td>3. In the Class name box, type the previously configured name of the expedited forwarding class—for example, <strong>ef-class</strong>.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong></td>
</tr>
</tbody>
</table>
Table 25: Assigning Forwarding Classes to Output Queues (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
| Configure an assured forwarding class classifier. | 1. Select Queue and click Add new entry.  
2. In the Queue num box, type 3.  
3. In the Class name box, type the previously configured name of the assured forwarding class—for example, af-class.  
4. Click OK. |

Related Topics
- Configuring CoS Classifiers (NSM Procedure) on page 37
- Configuring CoS Code Point Aliases (NSM Procedure) on page 39
- Configuring CoS Drop Profile (NSM Procedure) on page 41
- Configuring CoS Interfaces (NSM Procedure) on page 44
- Configuring CoS Rewrite Rules (NSM Procedure) on page 49
- Configuring CoS Schedulers (NSM Procedure) on page 52
- Configuring CoS and Applying Scheduler Maps on page 54

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 26 on page 45.
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 26: 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>1. Expand the <strong>Interfaces</strong> tree and select <strong>Interface</strong>. 2. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in Interface. 3. Enter the interface name in the Name box.</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>. 2. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in Interface. 3. Enter the comment for the interface in the Comment 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>. 2. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in Interface. 3. Enter the comment for the interface in the Comment 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>. 2. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in Interface. 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>. 2. Click the <strong>New</strong> button or select an interface and click the <strong>Edit</strong> button in Interface. 3. Select the scheduler map chassis from the list.</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. 2. Expand the <strong>Interface</strong> tree and select <strong>Input Traffic Control Profile</strong>. 3. Specify the comment and the profile name. 4. Click <strong>Ok</strong>.</td>
</tr>
<tr>
<td>Option</td>
<td>Function</td>
<td>Your Action</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Input Traffic Control Profile Remaining | Applies an input traffic scheduling and shaping profile for remaining traffic to the logical interface. | 1. Click the **New** button or select an interface and click the **Edit** button in Interface.  
2. Expand the **Interface** tree and select **Input Traffic Control Profile Remaining**.  
3. Specify a comment and a profile name.  
4. Click **Ok**. |
| Output Traffic Control Profile | Applies an output traffic scheduling and shaping profile to the logical interface. | 1. Click the **New** button or select an interface and click the **Edit** button in Interface.  
2. Expand the **Interface** tree and select **Output Traffic Control Profile**.  
3. Specify a comment and a profile name.  
4. Click **Ok**. |
| Output Traffic Control Profile Remaining | Applies an output traffic scheduling and shaping profile for remaining traffic to the logical interface. | 1. Click the **New** button or select an interface and click the **Edit** button in Interface.  
2. Expand the **Interface** tree and select **Output Traffic Control Profile Remaining**.  
3. Specify a comment and a profile name.  
4. Click **Ok**. |
| 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**. |
### Table 26: Interfaces Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| 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   |                                                                          |                                                                                                                                         |
| Name            | 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. |
| 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.   |
| 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**. |
### Table 26: Interfaces Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Excess Bandwidth Share</td>
<td>Sets the excess input bandwidth sharing value.</td>
<td>1. Expand the <strong>Interfaces</strong> tree and select <strong>Interface Set</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the <strong>New</strong> button or select an interface set and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Expand interface—set tree and select <strong>Input Excess Bandwidth Share</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Specify the comment and proportion.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Click <strong>Ok</strong>.</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. Expand the <strong>Interfaces</strong> tree and select <strong>Interface Set</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the <strong>New</strong> button or select an interface set and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Expand interface—set tree and select <strong>Input Traffic Control Profile</strong>.</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 <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. Expand the <strong>Interfaces</strong> tree and select <strong>Interface Set</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the <strong>New</strong> button or select an interface set and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Expand interface—set tree and select <strong>Input Traffic Control Profile Remaining</strong>.</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 <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. Expand the <strong>Interfaces</strong> tree and select <strong>Interface Set</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click the <strong>New</strong> button or select an interface set and click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Expand interface—set tree and select <strong>Output Traffic Control Profile</strong>.</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 <strong>Ok</strong>.</td>
</tr>
</tbody>
</table>
Table 26: 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 Remaining</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. 2. Click the New button or select an interface set and click the Edit button. 3. Expand interface—set tree and select Output Traffic Control Profile Remaining. 4. Specify the comment and profile name. 5. Click Ok.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring CoS Classifiers (NSM Procedure) on page 37
- Configuring CoS Code Point Aliases (NSM Procedure) on page 39
- Configuring CoS Drop Profile (NSM Procedure) on page 41
- Configuring CoS Forwarding Classes (NSM Procedure) on page 43
- Configuring CoS Rewrite Rules (NSM Procedure) on page 49
- Configuring CoS Schedulers (NSM Procedure) on page 52
- Configuring CoS and Applying Scheduler Maps on page 54

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 27 on page 50.

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 27: Configuring and Applying Rewrite Rules**

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
| Configure rewrite rules for DiffServ CoS. | 1. Click **Configure** next to Rewrite Rules.  
2. Click **Add new entry** next to Dscp.  
3. In the Name box, type the name of the rewrite rules—for example, rewrite-dscps. |

| 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. |
Table 27: Configuring and Applying Rewrite Rules (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
| 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. |

| 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. |
Table 27: Configuring and Applying Rewrite Rules (continued)

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

Apply rewrite rules to an interface.

---

**Related Topics**

- Configuring CoS Classifiers (NSM Procedure) on page 37
- Configuring CoS Code Point Aliases (NSM Procedure) on page 39
- Configuring CoS Drop Profile (NSM Procedure) on page 41
- Configuring CoS Forwarding Classes (NSM Procedure) on page 43
- Configuring CoS Interfaces (NSM Procedure) on page 44
- Configuring CoS Schedulers (NSM Procedure) on page 52
- Configuring CoS and Applying Scheduler Maps on page 54

**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 28 on page 53.
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 28: Configuring Schedulers

<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>
<tr>
<td>Configure drop profile map</td>
<td>1. Click the Add New icon.</td>
</tr>
<tr>
<td></td>
<td>2. Select drop-profile-map</td>
</tr>
<tr>
<td></td>
<td>3. In the Loss Priority box, select the required loss priority—for example, high.</td>
</tr>
<tr>
<td></td>
<td>4. In the Protocol box, select the type of protocol—for example, any.</td>
</tr>
<tr>
<td></td>
<td>5. In the Drop Profile box, select the previously configured drop profile</td>
</tr>
<tr>
<td></td>
<td>6. Click OK</td>
</tr>
<tr>
<td>Specify the transmit rate.</td>
<td>1. Click the Add New icon.</td>
</tr>
<tr>
<td></td>
<td>2. Expand Transmit Rate</td>
</tr>
<tr>
<td></td>
<td>3. Select Rate</td>
</tr>
<tr>
<td></td>
<td>4. Under Rate, select the appropriate option:</td>
</tr>
<tr>
<td></td>
<td>■ To not specify transmit rate, select None.</td>
</tr>
<tr>
<td></td>
<td>■ To enforce a specific transmission rate, select rate and type the transmission rate that you want to enforce.</td>
</tr>
<tr>
<td></td>
<td>■ To specify a percentage of transmission capacity, select percent and type an integer from 1 through 100.</td>
</tr>
<tr>
<td></td>
<td>■ To specify the remaining transmission capacity, select remainder.</td>
</tr>
<tr>
<td></td>
<td>5. Click OK</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring CoS Classifiers (NSM Procedure) on page 37
- Configuring CoS Code Point Aliases (NSM Procedure) on page 39
- Configuring CoS Drop Profile (NSM Procedure) on page 41
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 29 on page 54.
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>Configure a scheduler map for DiffServ CoS.</td>
<td>1. Click Add new entry.</td>
</tr>
<tr>
<td></td>
<td>2. In the Name box, type the name of the scheduler map—for example,</td>
</tr>
<tr>
<td></td>
<td>diffserv-cos-map</td>
</tr>
<tr>
<td>Configure a best-effort forwarding class and scheduler.</td>
<td>1. Select Forwarding Class and click Add new entry.</td>
</tr>
<tr>
<td></td>
<td>2. In the Name box, type the name of the previously configured best-effort forwarding class—for example, be-class.</td>
</tr>
<tr>
<td></td>
<td>3. Select the previously configured best-effort scheduler—for example, be-scheduler</td>
</tr>
<tr>
<td></td>
<td>4. Click OK</td>
</tr>
</tbody>
</table>
Table 29: Assigning Forwarding Classes to Output Queues  (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure an expedited forwarding class</td>
<td>1. Select <strong>Forwarding Class</strong> and click <strong>Add new entry</strong>.</td>
</tr>
<tr>
<td>and scheduler.</td>
<td>2. In the Name box, type the name of the previously configured expedited forwarding class—for example, ef-class.</td>
</tr>
<tr>
<td></td>
<td>3. Select the previously configured expedited forwarding scheduler—for example, ef-scheduler.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

| Configure an assured forwarding class     | 1. Select **Forwarding Class** and click **Add new entry**. |
| and scheduler.                            | 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**.                                                                                                                        |

| 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 37
- Configuring CoS Code Point Aliases (NSM Procedure) on page 39
- Configuring CoS Drop Profile (NSM Procedure) on page 41
- Configuring CoS Forwarding Classes (NSM Procedure) on page 43
- Configuring CoS Interfaces (NSM Procedure) on page 44
- Configuring CoS Rewrite Rules (NSM Procedure) on page 49
- Configuring CoS Schedulers (NSM Procedure) on page 52
Part 3
Managing J-series Services Routers and SRX-series Services Gateways

- Using System Management Features in J-series Services Routers and SRX-series Services Gateways on page 59
- Topology Manager on page 63
Chapter 8
Using System Management Features in J-series Services Routers and SRX-series Services Gateways

Managing J-series and SRX-series Device Software Versions Overview on page 59
Viewing and Reconciling Device Inventory Overview on page 59
Viewing Device Inventory in NSM (NSM Procedure) on page 60
Removing a J-series or SRX-series Device from NSM Management (NSM Procedure) on page 61

Managing J-series and SRX-series Device Software Versions Overview

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

When a software upgrade is applied to a J-series or SRX-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 J-series and SRX-series devices with dual Routing Engines.

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

Related Topics
- Viewing Device Inventory in NSM (NSM Procedure) on page 60
- Viewing and Reconciling Device Inventory Overview on page 59

Viewing and Reconciling Device Inventory Overview

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 J-series and SRX-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 J-Web 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**
- Viewing Device Inventory in NSM (NSM Procedure) on page 60

---

**Viewing Device Inventory in NSM (NSM Procedure)**

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.

To view the device inventory in NSM:

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 appears.
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.
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.
Removing a J-series or SRX-series Device from NSM Management (NSM Procedure)

Deleting a device removes all device configuration information from the management system, but might be the best solution if you need to perform extensive troubleshooting or reconfigure the device locally.

To remove a J-series or SRX-series device from NSM management:

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab and then select the device that you want to remove from NSM management.
3. Right-click and select Delete, or click the Delete button. The Delete dialog box appears. If the device is referenced in a firewall rule, this dialog box displays the rules that reference it. You can click the links that appear to display the security policies to view or edit those references.
4. Remove the device by clicking Next. The Delete dialog box displays the progress of the deletion.
5. After NSM finishes, click Finish to close the dialog box.

Related Topics

- Adding J-series Services Routers or SRX-series Services Gateways in NSM Overview on page 8
Chapter 9

Topology Manager

Overview of the NSM Topology Manager on page 63
Requisites for a Topology Discovery Overview on page 63
Understanding the NSM Topology Manager Toolbar on page 64

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 Overview on page 63
Understanding the NSM Topology Manager Toolbar on page 64

Requisites for a Topology Discovery Overview

To use the Topology Manager, first add one or more devices 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:

- The management IP address of the device that acts as the seed IP address.
- SNMP credentials:
  - For SNMPv1 and SNMPv2c: Community string.
  - For SNMPv3: Username, security level, authentication type, privacy type, privacy password, and authentication password.
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 63
- Understanding the NSM Topology Manager Toolbar on page 64

---

## Understanding 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**: Use this tool to print a network topology map as an image file and the devices and links tables as text files from different views.

- **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 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 63
Requisites for a Topology Discovery Overview on page 63
Part 4
Monitoring J-series Services Routers and SRX-series Services Gateways

- Real Time Monitoring of J-series Services Routers and SRX-series Services Gateways on page 69
Realtime Monitor Overview

The Realtime Monitor module in NSM includes views that you can use to monitor real-time status and statistics about all the managed security devices, VPN tunnels, NSRP clusters, IDP sensors, and IDP clusters in your network. You can also use the Realtime Monitor to identify problems, track security events, 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, and then color-coding each event to organize problems.

Related Topics

- Realtime Monitor Overview on page 69
- Viewing Device Status on page 70
Viewing Device Status

Table 30 on page 70 lists and describes device information that you can view through the Device Monitor.

<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>
<tr>
<td>Config Status</td>
<td>Current configuration status of the device in NSM:</td>
</tr>
<tr>
<td></td>
<td>■ None—No state has been set (does not show in Device Monitor).</td>
</tr>
<tr>
<td></td>
<td>■ Modeled—The device exists in NSM, but a connection to the device has not yet been established.</td>
</tr>
<tr>
<td></td>
<td>■ RMA—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></td>
<td>■ Waiting for 1st connect—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></td>
<td>■ Import Needed—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></td>
<td>■ OS Version Adjustment Needed—The firmware version detected running on the device is different from 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></td>
<td>■ Platform Mismatch—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></td>
<td>■ Device Firmware Mismatch—The OS version selected when adding a DMI device does not match the OS version running on the device itself.</td>
</tr>
<tr>
<td></td>
<td>■ Device Type Mismatch—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></td>
<td>■ Detected duplicate serial number—The device has the same sequence number as another managed device. A device in this state cannot connect to NSM.</td>
</tr>
<tr>
<td></td>
<td>■ Update Needed—An update to this device is required.</td>
</tr>
<tr>
<td></td>
<td>■ Managed—The device is currently being managed by NSM.</td>
</tr>
<tr>
<td></td>
<td>■ Managed, In Sync—The physical device configuration is synced with the modeled configuration in NSM.</td>
</tr>
</tbody>
</table>
### Table 30: Device Status Information (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
</table>
| Config Status (continued)      | ■ 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).  
■ 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).  
■ 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.  
■ 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. |
| Connection Status              | Connection status of the device in NSM:                                                                                                                                                                      |
|                                | ■ Up—Device is currently connected to NSM.                                                                                                                                                                  |
|                                | ■ Down—Device is not currently connected to NSM but has connected in the past.                                                                                                                              |
|                                | ■ Never Connected—Device has never connected to NSM.                                                                                                                                                        |
|                                | 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 devDaemon.deviceHeartbeatTimeout parameter in the Device Server configuration file. Refer to the Network and Security Manager Installation Guide for more information on editing configuration files. |
|                                | **NOTE:** 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. |
| Alarm                          | Displays the current alarm status for each device in NSM:                                                                                                                                                   |
|                                | ■ If device has any alarms, the most severe alarm severity is displayed (either Major or Minor).                                                                                                              |
|                                | ■ None—The device has no alarms.                                                                                                                                                                            |
|                                | ■ Unknown—The device status is unknown. For example, the device might not be connected.                                                                                                                                 |
|                                | ■ N/A—The device’s alarm is not pollable or discoverable, for example, this column shows “N/A” for ScreenOS and IDP devices.                                                                                  |
|                                | Alarm is colored:                                                                                                                                                                                           |
|                                | ■ Red for Major.                                                                                                                                                                                            |
|                                | ■ Orange for Minor.                                                                                                                                                                                          |
|                                | ■ Green for Ignore, None, Unknown, or N/A.                                                                                                                                                                  |
Table 30: 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>■ In Sync</td>
<td>The inventory information in the NSM database is synchronized with the information on the device.</td>
</tr>
<tr>
<td>■ Out Of Sync</td>
<td>The inventory information in the NSM database is not synchronized with the information on the device.</td>
</tr>
<tr>
<td>■ N/A</td>
<td>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>■ In Sync</td>
<td>The inventory information in the NSM database is synchronized with the software on the device.</td>
</tr>
<tr>
<td>■ Out Of Sync</td>
<td>The inventory information in the NSM database is not synchronized with the software on the device.</td>
</tr>
<tr>
<td>■ N/A</td>
<td>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>■ In Sync</td>
<td>The inventory information in the NSM database is synchronized with the licenses on the device.</td>
</tr>
<tr>
<td>■ Out Of Sync</td>
<td>The inventory information in the NSM database is not synchronized with the licenses on the device.</td>
</tr>
<tr>
<td>■ N/A</td>
<td>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

- Viewing Device Monitor Alarm Status (NSM Procedure) on page 72
- Configuring the Polling Interval for Device Alarm Status (NSM Procedure) on page 73

Viewing Device Monitor Alarm Status (NSM Procedure)

Alarms refresh automatically through periodic polling.

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. Retrieve the current alarm status in the device by clicking the Refresh button.
Configuring the Polling Interval for Device Alarm Status (NSM Procedure)

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

1. In the NSM navigation tree, select Device Manager > Devices.
2. Click the Device Tree tab, and then double-click the device to set the polling interval.
3. Click the Info tab, and select Device Admin.
4. 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.
5. Click one:
   - OK—Saves the changes.
   - Cancel— Cancels the modifications.

Related Topics
- Viewing Device Status on page 70
- Viewing Device Monitor Alarm Status (NSM Procedure) on page 72
Part 5
Index

- Index on page 77
Index

**C**
classifiers
   CoS ................................................................. 37
code point aliases .................................................. 39
CoS classifiers ....................................................... 37
CoS code point aliases ............................................ 39
CoS drop profiles .................................................. 41
CoS forwarding classes ........................................... 43
CoS interfaces ...................................................... 44
CoS rewrite rules .................................................. 49
CoS scheduler maps .............................................. 54
CoS schedulers .................................................... 52
customer support .................................................. xiii
   contacting JTAC .................................................. xiii

**D**
drop profiles ....................................................... 41

**F**
forwarding classes ............................................... 43

**R**
rewrite rules ....................................................... 49

**S**
scheduler maps ................................................... 54
   schedulers ....................................................... 52
support, technical See technical support

**T**
technical support
   contacting JTAC .................................................. xiii