

Intrusion Detection and Prevention IDP 4.1r4 Release Notes

Build 4.1.134028
September 22, 2009
Revision 02

Contents

Overview	2
Supported Hardware	2
Changed Features	2
IDP OS Directory Structure	2
Appliance Configuration Manager (ACM)	3
Network and Security Manager	4
Supported Upgrade Paths	4
Downgrading or Reverting	5
Licensing	5
Compatibility with Network and Security Manager	5
Browser Requirements	7
Upgrading IDP Software	7
Upgrading with NSM	8
Upgrading with the CLI	10
Resolved Issues	11
Known Issues	13
Documentation	14
Getting Help	15

Overview

Juniper Networks Intrusion Detection and Prevention Series devices enable you to enforce a security policy that protects your network from attacks and gather information about applications, clients, and servers in your network.

These release notes contain information about what is included in this product release: supported features, unsupported features, changed features, known problems, and resolved problems. If the information in the release notes differs from the information found in the documentation set, follow the release notes.

Supported Hardware

IDP 4.1r4 is supported on the following platforms:

- IDP75, IDP250, IDP800
- IDP50, IDP200, IDP600, IDP1100
- IDP10, IDP100, IDP500, IDP1000

Changed Features

In IDP 4.1r2, we introduced a feature to enable users to make a choice on how packet logs are forwarded from IDP to NSM:

- You could have the IDP device send packet capture logs to NSM as an integral part of the event log. This uses more bandwidth in communication between the IDP device and NSM and requires greater storage on the NSM server.
- You could have the IDP device send a unique ID to NSM that referred to the location of the packet capture file on the IDP device. In this second case, NSM requests the packet log from the IDP device only when you use the NSM Log Viewer to display a packet log. This uses less bandwidth and requires greater storage on the IDP device.

In IDP 4.1r4, we have made the following change related to this feature: we have changed the way the IDP device stores packet capture logs locally. Please familiarize yourself with the following changes:

- IDP OS Directory Structure on page 2
- Appliance Configuration Manager (ACM) on page 3
- Network and Security Manager on page 4

IDP OS Directory Structure

We have changed the directory structure for stored packet logs. Network administrators who use scripts and utilities to copy logs from the IDP device to a remote storage location should make note of the new structure.

Previously, packet capture logs were stored in `/usr/idp/device/var/pktlogs/`.

In IDP 4.1r4, packet capture logs are stored in numbered directories: `/usr/idp/device/var/pktlogs/0/`, `/usr/idp/device/var/pktlogs/1/`, `/usr/idp/device/var/pktlogs/2/`, and so forth. Each directory stores 100,000 logs. The total number of directories is determined by the value for Packet Log Count set with the Appliance Configuration Manager (ACM). For example, if you retain the default (10,000), all packet logs are stored in `/usr/idp/device/var/pktlogs/0/`. If you set Packet Log Count to 200,000, packet logs are stored two directories: `/usr/idp/device/var/pktlogs/0/` and `/usr/idp/device/var/pktlogs/1/`.

The first 100,000 packet capture logs are stored in `/usr/idp/device/var/pktlogs/0/`. Files are named `1.pcap`, `2.pcap`, ..., `100000.pcap`. The next 100,000 logs are stored in `/usr/idp/device/var/pktlogs/1/`. Files are named `1.pcap`, `2.pcap`, ... `100000.pcap`. The log agent continues to create directories and files in this manner until the user-specified limit is reached or the disk usage for the partition reaches 90% capacity.

When the *user-specified limit* is reached, the log agent begins overwriting packet log files, beginning with `/usr/idp/device/var/pktlogs/0/1.pcap`.

When the *disk limit* is reached:

1. The log agent deletes all 100,000 logs in the first directory, `/usr/idp/device/var/pktlogs/0/`, in order to reuse the directory and disk space.
2. The next logs are written to `/usr/idp/device/var/pktlogs/0/` and the files are named `1.pcap`, `2.pcap`, ..., `100000.pcap`.
3. When the limit is reached again, the log agent deletes all of the logs in the next directory, `/usr/idp/device/var/pktlogs/1/`. It continues writing in the current directory until it reaches 100,000.pcap.
4. Then, it begins writing in the next directory, which had been emptied in the previous step.

Appliance Configuration Manager (ACM)

You use ACM to configure the Packet Log Count—the maximum number of packet logs stored on the IDP device. The following configuration guidelines supersede the guidelines provided in the ACM online help:

- Default: 10,000
- Minimum: 100
- Maximum: 102,400,000 (You can specify a larger value up to the limit for an unsigned integer – 4,294,967,296; however, any value you specify greater than 102,400,000 is resolved to 102,400,000.)
- Special value: 0 specifies the maximum (102,400,000)



NOTE: Previously, 0 specified the limit for an unsigned integer value – 4,294,967,296. In 4.1r4, 0 specifies the actual maximum – 102,400,000.



NOTE: Be careful when modifying the Packet Log Count limit. If you first configure a large limit and later configure a smaller limit, you might delete directories of logs. For example, suppose you first set a Packet Log Count of 1,000,000. The log agent begins storing logs in up to 10 log directories. Later, you change the Packet Log Count to 100,000. The log agent cleans up the previous configuration, deleting unnecessary directories 1-9. Before you change the setting to a lower value, be sure you have copied all the logs you want saved to a remote location.



NOTE: You might encounter unexpected behavior if the following circumstances apply:

- You use ACM to change the Packet Log Count to a lower value—from 200,000 to 100,000, for example.
- At the same time, the agent process is handling requests from NSM for logs from `/usr/idp/device/var/pktlogs/` subdirectories.

In the typical case, we expect the agent to mark unnecessary subdirectories for deletion and clean them up after the Packet Log Count setting is applied. If the agent has locked a subdirectory marked for deletion in order to retrieve files for NSM, it will not delete the subdirectory.

Network and Security Manager

In NSM Device Manager, if you select **Report > Include Packet Data in Log**, the IDP device sends the packet log whenever it sends the rule-matching event log to NSM (this is the default). If you deselect **Include Packet Data in Log**, the IDP device sends only a reference to the packet capture file with the event log sent to NSM. In this second case, NSM requests the packet log from the IDP device only when you use the NSM Log Viewer to display a packet log.

Because the upgrade deletes the current packet log collection, the references to packet capture files within logs *collected by NSM prior to upgrade* will become invalid. When you use the NSM Log Viewer to display the earlier packet logs, NSM will return the following error: **Packet log not found**.

The upgrade does not affect the expected behavior for packet captures previously sent to NSM (that is, where you had selected **Include Packet Data in Log**) or the expected behavior for packet capture references collected after the upgrade.

Supported Upgrade Paths

You can upgrade directly from any of the following versions:

- 4.1r3
- 4.1r2a

To upgrade from earlier versions, you must first upgrade to 4.1r3 or 4.1r2a.

Downgrading or Reverting

You cannot downgrade or revert to a previous version. You can reimage the operating system, if necessary. For details on reimaging, see the installation guide.

Licensing

The upgrade procedure preserves your earlier license configuration. Reimaging does not. If you reimage the appliance, see the installation guide for information on licensing.

Compatibility with Network and Security Manager

At the time of the IDP 4.1r4 release, we verified compatibility with the following releases of Network and Security Manager (NSM):

- NSM 2008.2r2
- NSM 2007.3r5

NSM 2008.1 and 2007.3 require a schema update to support IDP75, IDP250, and IDP800. The schema update is also known as forward support.

To download and install a schema update:

1. Download the schema update software:
 - a. Go to <https://www.juniper.net/customers/csc/software/> and log in with your customer user name and password.
 - b. Navigate to **IDP > ScreenOS Software Downloads (including NSM/Global Pro, STRM, IDP and NetScreen-Remote) > Network and Security Manager > Version**, where *Version* is 2008.2, 2008.1, or 2007.3 (depending on your NSM release).
 - c. On this page, locate your NSM release number and download a corresponding pair of schema update files.

NSM Release	Download
2008.2	N/A – no schema update required.
2008.1r2	<ul style="list-style-type: none"> ■ server: nsm2008.1r2_schema_update_server.zip ■ client: nsm2008.1r2_schema_update_ui_win.zip or nsm2008.1r2_schema_update_ui_linux.zip
2008.1r1	<ul style="list-style-type: none"> ■ server: nsm2008.1r1_schema_update_server.zip ■ client: nsm2008.1r1_schema_update_ui_win.zip or nsm2008.1r1_schema_update_ui_linux.zip
2007.3r5	<ul style="list-style-type: none"> ■ server: nsm2007.3r5_schema_update_server.zip ■ client: nsm2007.3r5_schema_update_ui_win.zip or nsm2007.3r5_schema_update_ui_linux.zip
2007.3r4	<ul style="list-style-type: none"> ■ server: nsm2007.3r4_schema_update_server.zip ■ client: nsm2007.3r4_schema_update_ui_win.zip or nsm2007.3r4_schema_update_ui_linux.zip
2007.3r3	<ul style="list-style-type: none"> ■ server: nsm2007.3r3_schema_update_server.zip ■ client: nsm2007.3r3_schema_update_ui_win.zip or nsm2007.3r3_schema_update_ui_linux.zip
2007.3r2	<ul style="list-style-type: none"> ■ server: nsm2007.3r2_schema_update_server.zip ■ client: nsm2007.3r2_schema_update_ui_win.zip or nsm2007.3r2_schema_update_ui_linux.zip

2. Install the server schema update on the NSM server:
 - a. Log in to the NSM server host computer as root.
 - b. Copy the NSM server schema update file to a temporary location. We recommend `/tmp`.
 - c. Unzip the schema update. For example, type the following command:

```
unzip nsmreleasename_schema_update_server.zip
```

Where *releasenum* is a specific NSM release number, such as 2007.3r5, or 2008.1r2.

- d. Run the schema update. For example, type the following command:

```
sh nsmreleasenum_schema_update_server.sh
```

Where *releasenum* is a specific NSM release number, such as 2007.3r5, or 2008.1r2.

The update begins automatically. During the update process, the installer stops and restarts the management system.

3. Install the client schema update on the NSM client computer:
 - a. Log in as an user with administrator privileges on the computer where you are installing the UI.
 - b. Copy the client schema update file to the same location where you have installed the UI.
 - c. Unzip the schema update.
 - d. Run the schema update:
 - If you are upgrading the UI on a Windows-based PC, double-click the installer executable.
 - If you are upgrading the UI on a Linux-based computer, launch it from a command line using the following command:

```
sh nsmreleasenum_schema_update_ui_linux.bin
```

Where *releasenum* is a specific NSM release number, such as 2007.3r5, or 2008.1r2.

4. To verify that you have installed the schema update properly, view the NSM UI client login window and verify that the installed version number has changed to reflect the update. You can also use the Help menu option to view the installed version number.

Browser Requirements

The Appliance Configuration Manager (ACM), QuickStart utility, and IDP Reporter have Web user interfaces. We have verified compatibility with the following browsers:

- Internet Explorer 7.x, 6.x
- Firefox 3.x, 2.x

Upgrading IDP Software

During upgrade, the IDP appliance is gracefully shut down. If you have configured bypass for traffic interfaces, you do not need to be concerned about traffic disruption.

If you have not configured bypass, you should plan to complete your upgrade at an appropriate time.

You can use NSM or the CLI to upgrade IDP software. You must use NSM to complete the IDP detector engine and attack object updates. This section provides the following upgrade workflows:

- Upgrading with NSM on page 8
- Upgrading with the CLI on page 10

Upgrading with NSM

This section describes a workflow for upgrading IDP software using only NSM.

Before you begin: Copy any packet logs you want saved from `/usr/idp/device/var/pktlogs/` to a remote location. The upgrade process will delete the current packet log collection in order to implement packet log storage changes in IDP 4.1r4. Previously collected packet capture logs will not be available to NSM. For details on the changes, see “Changed Features” on page 2.

To update IDP software:

1. Add the IDP software to the NSM GUI server.
2. Push the IDP software from the NSM GUI server to one or more IDP devices.

To add an IDP software image to the NSM GUI server:

1. Download the software image:
 - a. Go to <https://www.juniper.net/customers/csc/software/> and log in with your customer username and password.
 - b. Enter the IDP device serial number to display a view of applicable software releases available for download.
 - c. Click the applicable link to display the software download page.
 - d. Download the software to a location you can access from your NSM client.
2. From the NSM main menu, select **Tools > Software Manager** to display the Software Manager dialog box.
3. Click the **+** button to display the Open dialog box.
4. Select the IDP software image you just downloaded and click **Open** to add the software image to the NSM GUI server.



NOTE: Do not change the name of the image file. The image file name must be exactly the same as the filename you download from Juniper Networks web site.

5. Click **OK**.

To push the software image from the NSM GUI server to IDP devices:

1. From the NSM main menu, select **Devices > Software > Install Device Software** to display the Install Device Software dialog box.
2. From the Select OS Name list, select **ScreenOS/IDP**.
3. From the Select Software Image list, select the image file you just added to the NSM GUI server.
4. In the Select Devices list, select the IDP devices on which to install the software update.
5. Click **Next** and complete the wizard steps.
6. Select **Automate ADM Transformation** to automatically update the Abstract Data Model (ADM) for the device after NSM installs the update.



NOTE: If you clear this setting, the update is installed onto the device, but you cannot manage the device from NSM until the device ADM is updated.

7. Click **Finish** to display upgrade status in the Job Information dialog box.
8. When the upgrade finishes, click **Close** to exit the Job Information dialog box.

The software upgrade is complete.

Next Steps:

1. Check to see if J-Security Center has released an update for the detector engine or attack database:

From the NSM main menu, select **Tools > View/Update NSM attack database** and complete the wizard steps.

2. Push the updated IDP detector engine to IDP devices:

From the NSM main menu, select **Devices > IDP Detector Engine > Load IDP Detector Engine for ScreenOS** and complete the wizard steps.



NOTE: Updating the IDP detector engine on a device does not require a reboot of the device.

3. Push a security policy update job to update attack objects in use in your security policy:
 - a. In NSM, select **Devices > Configuration > Update Device Config**.
 - b. Select devices to which to push the updates and set update job options.
 - c. Click **OK**.

Upgrading with the CLI

This section describes a workflow where you use the CLI to upgrade the software image on the IDP device. You still use NSM to update the detector engine and attack objects.

Before you begin: Copy any packet logs you want saved from `/usr/idp/device/var/pktlogs/` to a remote location. The upgrade process will delete the current packet log collection in order to implement packet log storage changes in IDP 4.1r4. Previously collected packet capture logs will not be available to NSM. For details on the changes, see “Changed Features” on page 2.

To upgrade IDP software from the CLI:

1. Download the software image to a host that runs an FTP server. Follow these steps:
 - a. Go to <https://www.juniper.net/customers/csc/software/> and log in with your customer username and password.
 - b. Navigate to **IDP > ScreenOS Software Downloads (including NSM/Global Pro, STRM, IDP and NetScreen-Remote)**. In the row for IDP, click **4.1**.
 - c. Download the **sensor_4_1r4.sh** file.
2. Connect to the IDP command-line interface in one of the following ways:
 - Use SSH to connect to the IP address or hostname for the management interface. Log in as **admin** and enter **su -** to switch to **root**.
 - If you prefer, make a connection through the serial port and log in as **root**.



NOTE: To make an SSH connection, you must have enabled SSH for the management port (eth0). For details, see the ACM online Help.

3. Use SCP or FTP to copy the software image file to the IDP appliance. The IDP appliance does not run an FTP server, so you have to initiate the FTP session from the IDP appliance.
4. Run the upgrade script by entering **sensor_4_1r4.sh**. When the script has finished, enter **reboot**.
5. In the NSM Device Manager, right-click the device, select **Adjust OS Version**, and complete the wizard steps.

The software upgrade is complete.

- Next Steps:**
1. Check to see if J-Security Center has released an update for the detector engine or attack database:

From the NSM main menu, select **Tools > View/Update NSM attack database** and complete the wizard steps.

2. Push the updated IDP detector engine to IDP devices:

From the NSM main menu, select **Devices > IDP Detector Engine > Load IDP Detector Engine for ScreenOS** and complete the wizard steps.



NOTE: Updating the IDP detector engine on a device does not require a reboot of the device.

3. Push a security policy update job to update attack objects in use in your security policy:
 - a. In NSM, select **Devices > Configuration > Update Device Config**.
 - b. Select devices to which to push the updates and set update job options.
 - c. Click **OK**.

Resolved Issues

The following issues are resolved when you upgrade to IDP 4.1r4:

- PR 305434. In IDP 4.1r3 release notes, we reported that we had resolved an issue where high CPU during a policy push could unexpectedly trigger internal bypass. This issue was reopened and fixed in 4.1r4 with a more robust network driver. This issue might still occur when the CPU usage exceeds 90%. In IDP 5.0, the architectural changes have resolved this issue so that it is not seen at all.
- PR 390652. In IDP 4.1r3 release notes, we reported an issue with support for internal bypass on copper ports for IDP50/200/600/1100. This issue was addressed with the IDP 4.1j2 patch and does not appear in IDP 4.1r4.
- PR 397564. In IDP 4.1r3 release notes, we reported an issue with intermittent link flapping for IDP250 and IDP800 interfaces. This issue was addressed with the IDP 4.1j2 patch and does not appear in IDP 4.1r4.
- PR 399529. In IDP 4.1r3 release notes, we reported an issue where the peer port modulation (PPM) feature detected link status incorrectly, resulting in link flapping. This issue was addressed with the IDP 4.1j2 patch and does not appear in IDP 4.1r4.
- PR 400869. In IDP 4.1r3 release notes, we reported an issue when pushing an update that includes the VOIP:SKYPE:LOGIN-1 and VOIP:SKYPE:LOGIN-2 objects. The update had failed with error “Missing member “VOIP:SKYPE:LOGIN-1”. This issue was addressed with the IDP 4.1j2 patch and does not appear in IDP 4.1r4.

- PR 401177. In IDP 4.1r3 release notes, we reported high CPU in some IDP800 deployments. We have resolved this issue in IDP 4.1r4.
- PR 406411. Resolved an issue with the way the application identification feature handles RSH traffic, which had resulted in a crash.
- PR 407270. Resolved an issue with the agent process that had resulted in connection failures between the IDP device and NSM.
- PR 424795. Resolved an issue with the peer port modulation feature. Immediately after the feature was enabled or disabled, the link speed for traffic interfaces configured for auto-negotiation would fall from 1 Gbps to 100 Mbps.
- PR 426869. Resolved an issue with the nicBypass logging. Previously, when the link state changed to nicBypass, the logs were not getting written to nicBypass logs.
- PR 432575. The event severity reported in syslog logs is now the same as NSM logs.
- PR 443972. Resolved an issue where the Recommended action coded in a protocol anomaly object was not the action taken.
- PR 450877. We have developed a performance analysis tool that measures the performance impact of attack objects or attack groups. For details, contact JTAC.
- PR 451461. Resolved an issue with process termination that had resulted in a crash when applying certain configuration changes with ACM or stopping and restarting a IDP process.
- PR 455312. For IDP 4.1r4, Juniper Networks QA has tested IDP Reporter version 1.0.29, which is included in the IDP 4.1r4 software image. IDP Reporter 1.0.29 resolves the following reported issues:
 - PR 297270. We have verified that IDP Reporter is now compatible with Mozilla Firefox 3.0.
 - PR 307900. Resolved an issue with IDP Reporter where the Top Activities report displayed “No data available.”
 - PR 422150. Resolved an issue with IDP Reporter CPU and memory utilization reports.
 - PR 438169. Resolved an issue where the date/time and DNS changes set with ACM were not applied to IDP Reporter.
 - PR 458336. Resolved an issue that caused a delay in populating IDP Reporter Application reports.
 - PR 459036. Resolved an issue with the IDP Reporter Network reports. The Packets Received and Bytes Received counts were incorrect.
- PR 461900. We have made changes to packet log storage. For details, see “Changed Features” on page 2

Known Issues

The following issues are present in IDP 4.1r4:

- PR 227241. In IDP 4.1r3 release notes, we reported an issue with OS fingerprint reports in NSM – NSM reports “Unknown OS” for some types of destination servers. IDP 4.1r4 does not resolve this issue.
- PR 274963, 308133. In IDP 4.1r3 release notes, we reported that the following I/O modules do not support peer port modulation (PPM) on IDP800:
 - 4-port, 1 GigE fiber SFP (without bypass) (IDP-1GE-4SFP)
 - 4-port, 1 GigE fiber SX (with bypass) (IDP-1GE-4SX-BYP)

IDP 4.1r4 does not resolve this issue.

- PR 303672. In IDP 4.1r3 release notes, we reported an issue with custom attack signatures. Negation inside case-insensitive block is not supported. IDP 4.1r4 does not resolve this issue. To work around this issue, rewrite the signature to avoid negation inside a case-insensitive block.
- PR 312767. In IDP 4.1r3 release notes, we reported a corner case where you might encounter error messages in the ACM Configuration Confirmation page under the following sequence of actions:
 1. Use ACM to configure IDP in sniffer mode. Apply and save the configuration.
 2. Use QuickStart to change to transparent mode. Apply and save the configuration.
 3. Use ACM to change to transparent mode. Apply and save the configuration.

IDP 4.1r4 does not resolve this issue. If you encounter this case through this sequence of actions, you can safely ignore the error messages.

- PR 455947. In the NSM Device Manager, when you select and right-click the device, the Software > Install Device Software submenu does not work as expected. You cannot use this navigation sequence to install the IDP 4.1r4 software. Instead, follow the procedures exactly as they are provided in “Upgrading with NSM” on page 8.
- PR 462005. IDP Reporter Application reports show incorrect statistics for bytes transferred. The report shows only client-to-server bytes, not total bytes.
- PR 474067. If you reimage the IDP device with the `sensor_4_1r4.iso` file, the `/usr/idp/device/bin/system_funcs` file is not created until you complete the EasyConfig wizard to set the initial network configuration. When reimaging, be prepared to run the EasyConfig wizard immediately after completing the reimaging procedure. For details on reimaging and running the EasyConfig wizard, see the installation documentation for your IDP device.

Documentation

You can download user documentation from the Juniper Networks Web site:
<http://www.juniper.net/techpubs/>.

Table 1 on page 14 lists related IDP documentation.

Table 1: Related IDP Documentation

Document	Description
IDP/ISG signature update announcements	Describes new pre-defined attack objects or modifications. Go to http://rss.juniper.net/p/subscribe to subscribe to signature update announcements.
IDP Detector Engine release notes	Provides information about new features, changed features, fixed problems, and known issues with the IDP Detector Engine release. You can download these release notes from the following location: http://www.juniper.net/techpubs/software/management/idp/de/index.html
JTAC Knowledge Base	Troubleshooting tips and troubleshooting workflows are published in the Juniper Networks Technical Assistance Center (JTAC) knowledge base at http://kb.juniper.net . To subscribe to an RSS feed for IDP-related KB articles, go to http://kb.juniper.net/index?page=content&cat=IDP_OS&channel=KB and click the RSS feed icon.
<i>IDP Installation Guide</i>	Describes IDP hardware and provides instructions for installing, configuring, updating, and servicing the device.
<i>IDP Administration Guide</i>	Provides procedures for completing IDP administration tasks with the Network and Security Manager (NSM) central management program; with the IDP device Appliance Configuration Manager (ACM); and with the IDP device command-line interface (CLI).
<i>IDP Concepts and Examples Guide</i>	Explains IDP features and provides examples of how to use the system.
<i>IDP Custom Attack Objects Reference and Examples Guide</i>	Provides examples and reference information for creating custom attack objects.
<i>IDP Reporter User's Guide</i>	Describes how to use IDP Reporter.

Table 1 on page 14 lists related NSM documentation.

Table 2: Related NSM Documentation

Document	Description
Network and Security Manager release notes	Provides information about new features, changed features, fixed problems, and known issues with the NSM release.

Table 2: Related NSM Documentation (continued)

Document	Description
<i>Network and Security Manager Configuring Intrusion Detection and Prevention Devices Guide</i>	Describes how to configure and manage IDP devices using NSM. This guide also helps in understanding of how to configure basic and advanced NSM functionality, including adding new devices, deploying new device configurations, updating device firmware, viewing log information, and monitoring the status of IDP devices.
<i>Network and Security Manager Installation Guide</i>	Describes how 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 to NSM.
<i>Network and Security Manager Administration Guide</i>	<p>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.</p> <p>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.</p>
Network and Security Manager Online Help	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.

Getting Help

If you need additional information or assistance, contact Juniper Networks Technical Assistance Center (JTAC) by E-mail (support@juniper.net) or telephone (1-888-314-JTAC within the United States or 1-408-745-9500 from outside the United States).

Copyright © 2009, Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.