Network and Security Manager
NSMXpress Quick Start

December 22, 2008
Part Number: 530-028103-02
Revision 1

NSMXpress is an appliance version of Network and Security Manager (NSM). NSMXpress simplifies the complexity of network administration by providing a single, integrated management interface that controls device parameters.

This robust hardware management system installs in minutes with full high availability (HA) support, making it easy to scale and deploy. Enterprise customers with limited resources can benefit significantly from NSMXpress by eliminating the need to have dedicated resources for maintaining a network and security management solution.

NSMXpress makes it easy for administrators to control device configuration, network settings, and security policy settings for multiple families of Juniper devices including:

- ScreenOS firewall/VPN devices and intrusion detection and prevention (IDP) devices
- JUNOS devices, such as J-series routers, SRX-series gateways, EX-series switches, M-series Internet routers, and MX-series Ethernet Services routers.
- Secure Access devices
- Unified Access Control (Infranet Controller) devices.

For a complete list of supported device families and platforms, see the Network and Security Manager Administration Guide.

Up to 10 administrators can log into NSMXpress concurrently.

This quick start explains the following steps for installing and configuring NSMXpress and for configuring NSM.
1. Install the NSMXpress appliance hardware.
2. Set up the NSMXpress appliance, using the serial port.
3. Configure the NSMXpress software, using the Web interface.
4. Configure NSM software, which was preinstalled onto the NSMXpress appliance, with site-specific parameters.

Contents

Hardware Installation ................................................................. 4
NSMXpress Ports ................................................................. 4
Installing the Hardware ............................................................. 5
Initial Setup Configuration ......................................................... 6
  Boot NSMXpress ............................................................... 7
  Set Up Your Appliance ......................................................... 7
  Web Interface Configuration .................................................. 8
Configuring the NSM Software .................................................. 8
  Configuring Basic Settings .................................................... 9
  Configuring High Availability ............................................... 11
  Advanced Options .............................................................. 14
    Enabling and Configuring Remote Replication of the Database ..... 15
    Enabling and Configuring SRS (Regional Server Only) ............. 16
Installing NSM Software ......................................................... 17
Managing NSM Administration .................................................. 18
  Changing the Superuser Password ......................................... 18
  Downloading NSM MIBS (Regional Server Only) .................... 18
  Exporting Audit Logs .......................................................... 19
  Exporting Device Logs (Regional Server Only) ......................... 19
  Generating Reports (Regional Server Only) ............................ 20
  Modifying NSM Configuration Files ....................................... 20
  Backing Up the NSM Database .............................................. 21
  Changing the NSM Management IP ......................................... 22
  Scheduling Security Updates ................................................ 22
Managing System Administration .............................................. 23
  Rebooting or Shutting Down NSMXpress .................................. 23
  Changing the User Password ................................................ 24
Configuring the Network ......................................................... 24
  Network Interfaces ............................................................. 25
  Routing and Gateways ......................................................... 25
  Hostname and DNS Clients .................................................. 26
  Host Addresses ................................................................. 26
Monitoring with SNMP ............................................................ 27
  SNMP Configuration .......................................................... 27
  SNMP System Information ................................................... 28
  SNMP Trap Configuration .................................................... 28
Forwarding Syslog Messages .................................................... 29
  Viewing Syslog Receivers .................................................... 30
  Adding and Configuring Syslog Receivers ............................... 31
  Editing Syslog Receiver Configurations ................................... 33
  Deleting Syslog Receivers .................................................... 33
Changing the System Time ....................................................... 33
**Hardware Installation**

We recommend that you install NSMXpress on your LAN to ensure that it can communicate with your applicable resources, such as authentication servers, DNS servers, internal Web servers through HTTP/HTTPS, external Web sites through HTTP/HTTPS (optional), the Juniper update server via HTTP, Network File System (NFS) file servers (optional), and client/server applications (optional).

---

**NOTE:** If you decide to install NSMXpress in your DMZ, ensure that it can connect to your internal resources.

---

**NSMXpress Ports**

Table 1 on page 4 provides required port information on the NSMXpress.

### Table 1: Required Ports on NSMXpress

<table>
<thead>
<tr>
<th>Direction</th>
<th>Port</th>
<th>Description</th>
<th>LAN</th>
<th>Internet</th>
<th>Depends on Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>In</td>
<td>22</td>
<td>SSH command-line management</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>443</td>
<td>Web interface for administrator login</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>8443</td>
<td>Web interface for listening for NSM API messages.</td>
<td>LAN</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>7800</td>
<td>Connections from managed devices to NSMXpress</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>7801</td>
<td></td>
<td>Connections from the NSM GUI to NSM</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>7802</td>
<td></td>
<td>Heartbeat between peers in an HA cluster</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>7803</td>
<td></td>
<td>Connections from managed IDP devices to NSM</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>7804</td>
<td></td>
<td>Connections from JUNOS devices, Secure Access devices, or Infranet Controller devices</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 1: Required Ports on NSMXpress (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>Port</th>
<th>Description</th>
<th>LAN</th>
<th>Internet</th>
<th>Depends on Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out</td>
<td>22</td>
<td>SSH connection to new managed device</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>23</td>
<td>Telnet connection to new managed device</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>53</td>
<td>DNS lookups</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>80</td>
<td>System Security Updates from Juniper Networks</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>111</td>
<td>Shared Disk portmap lookup</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>123</td>
<td>Network Time Protocol (NTP) time synchronization</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>2049</td>
<td>Shared Disk NFS connection</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

For more information on ports, refer to the Network and Security Manager Installation Guide.

Installing the Hardware

Follow these steps to unpack the NSMXpress appliance and connect it to your network.

To install NSMXpress:
1. Place the shipping container on a flat surface and remove the hardware components with care.
2. Remove the NSMXpress device from the shipping container and place it on a flat surface.
3. Mount NSMXpress in your server rack using the attached mounting brackets.
4. Plug the power cord into the AC receptacle on the rear panel.
   - If your NSMXpress contains two power supplies, plug a power cord into each AC receptacle.
5. Plug the other end of the power cord into a wall socket.
   - If your NSMXpress contains two power supplies, plug each power cord into a separate power circuit to ensure that the NSMXpress continues to receive power if one of the power circuits fails.
6. Plug the Ethernet cable into the port marked ETH0 on the front panel. See Figure 1 on page 6.
7. Plug the null modem serial cable into the console port. See Figure 1 on page 6.

This cable was shipped with your NSMXpress. If you do not have this cable, use any other null modem serial cable.

8. Push the power button in the upper left corner of the front panel.

The green LED below the power button turns on. The NSMXpress hard disk LED turns on whenever the appliance reads data from or writes data to an NSMXpress hard disk.

The internal port uses two LEDs to indicate the LAN connection status, which is described in Table 2 on page 6.

Hardware installation is now complete. The next step is to set up the software, as described in “Initial Setup Configuration” on page 6.

Table 2 on page 6 provides LED information for the ETH0 and ETH1 ports.

**Table 2: Ethernet Port LEDs**

<table>
<thead>
<tr>
<th>LAN Status</th>
<th>LED 1</th>
<th>LED 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Mbps connection</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>100 Mbps connection</td>
<td>Green</td>
<td>Off</td>
</tr>
<tr>
<td>1000 Mbps connection</td>
<td>Orange</td>
<td>Off</td>
</tr>
<tr>
<td>Data is being transferred</td>
<td>Orange, Green, or Off</td>
<td>Blinking</td>
</tr>
<tr>
<td>No connection</td>
<td>Off</td>
<td>Off</td>
</tr>
</tbody>
</table>

**Initial Setup Configuration**

When you first turn on an unconfigured NSMXpress appliance, you need to enter basic network and machine information through the serial console to make your appliance accessible to the network. After entering these settings, you can continue configuring the appliance using the CLI or the Web interface. You are not prompted for the initial setup information again.
This section describes the required serial console setup and the tasks you need to perform when connecting to your NSM Xpress for the first time:

- Boot NSM Xpress on page 7
- Set Up Your Appliance on page 7

**Boot NSM Xpress**

To configure NSM Xpress for the first time, you must attach your NSM Xpress appliance to a console terminal running an emulation utility such as HyperTerminal.

1. Configure a console terminal or terminal emulation utility to use the following serial connection parameters:
   - 9600 bits per second
   - 8-bit no parity (8N1)
   - 1 stop bit
   - No flow control
2. Connect the terminal or laptop to the null modem serial cable plugged into the NSM Xpress console port.
3. Turn on the NSM Xpress appliance.

When NSM Xpress is powered on, the serial console displays diagnostic information before proceeding to the boot countdown. When complete, the serial console displays the login prompt terminal emulator.

```
NSMXpress.juniper.net login:
```

4. Enter `admin` as your default login name.
5. Enter `abc123` as your default password.
6. Change your default password when prompted. Enter the default password first, followed by your new password. All passwords are case sensitive.

**Set Up Your Appliance**

This section provides the minimum information necessary to make your appliance active on the network.

To set up your appliance either as a regional server or a central manager, follow these steps:

1. Enter the IP address for interface eth0 and press Enter.
2. Enter the subnet mask for interface eth0 and press Enter.
3. Enter the default route or default gateway address for interface eth0 and press Enter.
Applying changes...
Re-loading database
ip_tables: (C) 2000–2002 Netfilter core team
ip_tables: (C) 2000–2002 Netfilter core team
ip_tables: (C) 2000–2002 Netfilter core team
Done!

Your NSMXpress is now active on the network.
To configure your system via a web browser, connect to:
https://10.150.43.205/admin

To configure your system via command line, type:
nsm_setup

For operation of NSM server, switch to user “nsm”.
Please consult NSM product documentation for details.

To configure the NSM software using the CLI, see the NSMXpress User Guide. To configure the NSM software using the Web interface, go to “Web Interface Configuration” on page 8.

Web Interface Configuration

To configure NSM on your system from a Web interface, use the following steps.

1. Copy the URL (starting with https://) from the terminal emulator after installing NSMXpress:

   Your NSMXpress is now active on the network.
   To configure your system via a web browser, connect to:
   https://10.150.43.205/admin

2. Open a Web browser and paste the URL into the address text box.
3. Press Enter to open the NSMXpress login page.
4. Enter the admin user name and password and then click Login.
5. See “Configuring the NSM Software” on page 8 for details about how to install and configure NSM on your NSMXpress appliance from the Web interface.

Configuring the NSM Software

After logging in as an ‘admin’ user, an initial setup script walks you through additional configuration system settings before finalizing the NSM installation. This chapter describes that setup process.
Your NSMXpress appliance comes preconfigured as a regional server or a central manager. Most installation and configuration steps in this section are identical for both types of server. All exceptions are noted.

After logging into the NSMXpress Web interface, NSMXpress provides you with the following installation options:

- Configuring Basic Settings on page 9
- Configuring High Availability on page 11
- Advanced Options on page 14
- Installing NSM Software on page 17

**Configuring Basic Settings**

To install the regional server or central manager software using the minimum requirements:

1. Install your NSMXpress hardware as described in “Hardware Installation” on page 4.
2. Boot and setup your NSMXpress appliance as described in “Initial Setup Configuration” on page 6.
3. Enter the `https://<ip>/admin` URL for your appliance in a Web browser. See “Web Interface Configuration” on page 8 for details.
4. Log into the Web interface as an ‘admin’ user to open the Install NSM Regional Server window (see Figure 2 on page 10) or the Install NSM Central Manager window (see Figure 3 on page 10).

**NOTE:** The ‘admin’ user default username is admin and the password is the one you created in Step 6 of “Boot NSMXpress” on page 7.
### Figure 2: Regional Server Configuration Main Menu

**Install NSM Regional Server**

**NSM Configuration Main Menu**

<table>
<thead>
<tr>
<th>Management IP</th>
<th>172.24.68.111 C</th>
</tr>
</thead>
</table>

The IP address on this server that will be used for management.

**NSM 'super' password**

Password for 'super' user

**NSM License type**

Specify a license file, or select 'Base Install' to use the built-in limited device license.

**Remote Replication of Database**

Off

**High Availability**

Off

**SRS**

Off

Submit

Install

### Figure 3: Central Manager Configuration Main Menu

**Install NSM Central Manager**

**NSM Configuration Main Menu**

<table>
<thead>
<tr>
<th>Management IP</th>
<th>172.24.68.111 C</th>
</tr>
</thead>
</table>

The IP address on this server that will be used for management.

**NSM 'super' password**

Password for 'super' user

**Remote Replication of Database**

Off

**High Availability**

Off
5. Enter the primary IP address of your management server for eth0 (the default).

You can use the default IP address next to the first radio button or select the second radio button and then enter a different IP address. Each IP address you add (in addition to the default IP address) will be available in the drop-down list after you click the second radio button.

6. Enter the NSM superuser password in the top text box, and then reenter it in the text box below it.

This password must be at least eight characters long and is case sensitive. This password is used by the NSM superuser (also referred to as the NSM administrator). This user has the highest level of privileges in NSM.

7. Enter the GUI Server one-time password in the top text box, and then reenter it in the text box below it. This password is used to authenticate this NSM server with other NSM servers with which it communicates. Regional servers use this password to authenticate peer servers in an HA configuration and to authenticate the central manager. The central manager uses this password to authenticate its peer server in an HA configuration and any regional servers it manages. NSM servers must have the same GUI Server one-time password, or the authentication will fail.

8. Select the license option. (This option is available only for regional servers.)

   a. Select **Base Install** to use the built-in limited device license for as many as 25 devices.

   b. Click **Upload license file** to upload the license file you generated using the Juniper License Management System (LMS), which permits you to manage more than 25 devices. This license file must be located on your local hard drive.

      See the Network and Security Manager installation Guide for more information about NSM licensing.

9. Click **Submit** to save any changes, and then click **Install** to install the software.

**Configuring High Availability**

To configure high availability (HA) settings:
1. On the NSM Configuration Main Menu, click **Menu** next to High Availability to access HA options. See Figure 4 on page 12.

**Figure 4: High Availability Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High Availability</strong></td>
<td>n</td>
</tr>
<tr>
<td><strong>Primary Status</strong></td>
<td>y</td>
</tr>
<tr>
<td><strong>HA Remote IP</strong></td>
<td></td>
</tr>
<tr>
<td><strong>HA Link Failure Detection IP</strong></td>
<td></td>
</tr>
<tr>
<td><strong>HA Inter-server password</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Shared Disk</strong></td>
<td>Off</td>
</tr>
<tr>
<td><strong>HA Links</strong></td>
<td>Menu</td>
</tr>
<tr>
<td><strong>HA Advanced Settings</strong></td>
<td>Menu</td>
</tr>
</tbody>
</table>

2. Use the **High Availability** option to turn HA on (y) or off (n). The default is off.

3. Use the **Primary Status** option to set your NSMXpress appliance as either the primary or secondary server in the HA cluster. If you select y, it is the primary server (the default). If you select n, it is the secondary server.

4. Use the **HA Remote IP** option to enter the IP address for the HA peer in the HA cluster.

5. Use the **HA Link Failure Detection IP** option to enter the IP address of a computer outside the HA cluster that you can ping to verify connection status.

6. Use the **HA Inter-server password** option to enter the heartbeat password used between the primary and secondary servers.

7. Click **Submit** to save the changes.

8. Click **Menu** next to **Shared Disk** (see Figure 4 on page 12) to configure a shared disk for regional servers (see Figure 5 on page 13) or for central managers (see Figure 6 on page 13). This step is optional.
NSMXpress supports shared disk via NFS only. Due to the data-intensive nature of NSM, we recommend gigabit speed links (1000 Mbps) for shared disk use. For more information about custom settings, refer to the Network and Security Manager Installation Guide.

9. Click Menu next to HA Links (see Figure 4 on page 12) to configure the second link in the HA cluster (see Figure 7 on page 13). This step is optional.

Figure 7: HA Links Options

Use the options in this menu to set up a redundant link for the HA cluster. If you are going to use a second link, you need to set the IP address for eth1 before configuring this setting (see “Configuring the Network” on page 24 for details). Setting a redundant link is optional. For more information about custom settings, refer to the Network and Security Manager Installation Guide.
If you configure HA with just one heartbeat link, then device management traffic and data replication traffic both use that link. If you configure two links, device management traffic uses the first link and data replication uses the second.

If you set the HA link count to 2, an expanded menu appears to configure the second link:

![Figure 8: Redundant Links](image)

10. Click **Menu** next to HA Advanced Settings (see Figure 4 on page 12) to configure HA advanced settings (see Figure 9 on page 14). This step is optional.

For more information about custom settings, refer to the *Network and Security Manager Installation Guide*.

![Figure 9: HA Advanced Settings](image)

11. Click **Submit** to save the HA options and return to the NSM Configuration Main Menu.

**Advanced Options**

To display the Advanced Options menu, on the NSM Configuration Main Menu, select **Menu** next to Advanced Options. The Advanced Options menu appears as shown in Figure 10 on page 15.
Figure 10: Advanced Options Menu

<table>
<thead>
<tr>
<th>Menu: Advanced Options</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>https port for NBI service</td>
<td>8443</td>
<td>Off</td>
</tr>
<tr>
<td>Remote Replication of Database</td>
<td>Off</td>
<td>Menu</td>
</tr>
<tr>
<td>SRS</td>
<td>Off</td>
<td>Menu</td>
</tr>
</tbody>
</table>

Advanced installation options include:

- https port for NBI service—Allows you to configure a port to listen for messages for the NSM API. By default, this value is 8443. You can configure it to any port number from 1025 to 65535.

- Remote Replication of Database—Mirrors the daily backup to an external server. You can toggle it on or off. After you turn it on, use the menu options to configure this option.

- SRS Enabled Options (regional server only)—Opens a menu to enable and configure Statistical Report Server (SRS). These options enable NSMxpress to interface with SRS. You can toggle it on or off. When it is on, a menu with additional options is available.

NOTE: SRS must be installed on a separate server from NSM.

The following sections provide details about the remote replication and SRS options:

- Enabling and Configuring Remote Replication of the Database on page 15
- Enabling and Configuring SRS (Regional Server Only) on page 16

Enabling and Configuring Remote Replication of the Database

To configure remote replication of database settings:
1. On the Advanced Options menu, click **Menu** next to Remote Replication of Database (see Figure 4 on page 12) to configure daily backups (see Figure 11 on page 16).

**Figure 11: Remote Replication of Database Options**

<table>
<thead>
<tr>
<th>Remote Replication of Database</th>
<th>y</th>
<th>y</th>
</tr>
</thead>
<tbody>
<tr>
<td>If 'y', local backups will be sent to a remote backup machine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hour of day to Replicate Database</td>
<td>02</td>
<td>00</td>
</tr>
<tr>
<td>Hour to start a backup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Backup IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP address of a remote backup machine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Replication Timeout (seconds)</td>
<td>1800</td>
<td></td>
</tr>
<tr>
<td>Rsync Command Backup Timeout (seconds)</td>
<td>[Default is 1800 seconds] (Range is 1 to 65535)</td>
<td></td>
</tr>
</tbody>
</table>

2. Use the Remote Replication of Database option to turn remote replication on (y) or off (n). The default is off.

3. Use the Hour of day to Replicate Database option to start the backup. The valid range (in hours) is 00-23. The default is 2 AM.

4. Use the Remote Backup IP option to enter the IP address of the remote backup server.

   Backup information is copied to the `/var/netscreen/dbbackup` directory on the remote server. The ‘nsm’ user must exist on both servers and you must establish an SSH trust relationship. See the *Network and Security Manager Installation Guide*, for details.

5. Use the Remote Replication Timeout option to set up a timeout for Rsync. The valid range (in seconds) is 1-65535. The default is 1800 seconds.

6. Click **Submit** to save the options and return to the main menu or continue with the other advanced installation options.

**Enabling and Configuring SRS (Regional Server Only)**

This option is not available on central manager. To configure statistical report server (SRS) settings:

---

**NSMXpress Quick Start**
1. On the Advanced Options menu, click Menu next to SRS (see Figure 4 on page 12) to open the SRS menu (see Figure 12 on page 17).

**Figure 12: SRS Menu**

<table>
<thead>
<tr>
<th>Menu: SRS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SRS</strong></td>
</tr>
<tr>
<td>Statistical Report Server will be used on this GUI server.</td>
</tr>
<tr>
<td><strong>SRS DB IP</strong></td>
</tr>
<tr>
<td>Database server IP address.</td>
</tr>
<tr>
<td><strong>SRS DB Type</strong></td>
</tr>
<tr>
<td>Database type.</td>
</tr>
<tr>
<td><strong>SRS Database Name</strong></td>
</tr>
<tr>
<td>Database name.</td>
</tr>
<tr>
<td><strong>SRS DB Owner Name</strong></td>
</tr>
<tr>
<td>Database user name.</td>
</tr>
<tr>
<td><strong>SRS DB Owner Password</strong></td>
</tr>
<tr>
<td>Database password.</td>
</tr>
</tbody>
</table>

2. Use the SRS options to turn SRS on (y) or off (n). The default is off. If you turn on this feature, the server is used with the GUI server.

3. Use the SRS DB IP option to enter the IP address for the server on which you have installed the SRS database server.

4. Use the SRS DB Type option to select the database type. The values are pgsql (the default), oracle, or mssql.

5. Use the SRS Database Name option to enter the name of the SRS database. The default value is netscreen. To enter another name, click the radio button next to the blank text box and enter the name in the text box.

6. Use the SRS DB Owner Name option to enter the owner’s name of the SRS database. The default value is netscreen. To enter another name, click the radio button next to the blank text box and enter the name in the text box.

7. Use the SRS Database Owner Password option to enter the SRS database password. The password requires a minimum of eight characters and is case sensitive. Reenter it in the second text box.

8. Click Submit to save the options and return to the NSM Configuration Main Menu.

**Installing NSM Software**

After you submit all your configuration options, click Install to install the NSM software on your NSM Xpress appliance. Installation takes a few minutes. A status indicator
shows the progress of the installation. Wait until installation is finished before continuing to use the Web interface.

Managing NSM Administration

Expand **NSM Administration** in the left navigation tree to access the options described in this section. These options are available only after installing NSM.

The following sections explain how to use each of the NSM Administration options:

- Changing the Superuser Password on page 18
- Downloading NSM MIBS (Regional Server Only) on page 18
- Exporting Audit Logs on page 19
- Exporting Device Logs (Regional Server Only) on page 19
- Generating Reports (Regional Server Only) on page 20
- Modifying NSM Configuration Files on page 20
- Backing Up the NSM Database on page 21
- Changing the NSM Management IP on page 22
- Scheduling Security Updates on page 22

**Changing the Superuser Password**

To change the superuser password, select **NSM Administration > NSM Super User Password**. See Figure 13 on page 18.

**Figure 13: Change Superuser Password**

![Change Password for Super User](image)

**Downloading NSM MIBS (Regional Server Only)**

To download any available MIBs, select **NSM Administration > Download NSM MIBS**, and then click **Download MIB**. See Figure 14 on page 19. This option is not available on central manager.
Exporting Audit Logs

To export audit logs, select **NSM Administration** > **Export Audit Logs**. See Figure 15 on page 19.

To export an audit log to a csv file, select **csv** in the drop-down list box, and then enter the csv file name in the text box.

To export an audit log to a syslog server, select **syslog** in the drop-down list box, and then enter the server IP address, if it is not the local host.

Exporting Device Logs (Regional Server Only)

To export device logs, select **NSM Administration** > **Export Device Logs**. See Figure 16 on page 19). This option is not available on central manager.
Generating Reports (Regional Server Only)

To generate reports, select **NSM Administration > Generate Reports**. See Figure 17 on page 20. This option is not available on central manager.

**Figure 17: Generate Reports**

<table>
<thead>
<tr>
<th>Domain:</th>
<th>Type:</th>
<th>Report:</th>
<th>Script:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eg: global</td>
<td>Eg: system/shared</td>
<td>Eg: mytest</td>
<td>Eg: Ap.sh/email.sh</td>
</tr>
</tbody>
</table>

**NOTE:** The user is an NSM administrator and not an NSMXpress user. Enter a user name as domain/user, such as `global/super`.

Modifying NSM Configuration Files

To manually edit the `GuiSrv.cfg`, `DevSrv.dfg`, and `HaSrv.cfg` files, select **NSM Administration > Modify NSM Configuration Files**. The example in Figure 18 on page 21, shows the option to modify the `GuiSrv.cfg` file.
Figure 18: NSM Configuration Files

NSM Configuration Files

GuiSvc.cfg

The page allows you to manually edit the /var/netscreen/GuiSvc/var/guiSvc.cfg. Be careful, as no syntax checking will be done on your edits.

The server will be restarted once the changes are made.

```bash
# this file contains just enough info for the processes
# to start up. Each process should pull its complete
# configuration from the XML DB

setuid.user               NSM
clientId                  0
peerGuiSvcId              3
clientOneTimePassword     dS30S6

default.printLevel        warn
Default.printProperties   where=file, sync=0, maxfilenum=15
#statusMonitor.printLevel debug
#statusMonitor.printProperties where=file, sync=1, maxfilenum=150
#guiSvcDirectiveHandler.printLevel debug
#guiSvcLicenseManager.printLevel debug
#guiSvcLicenseManager.licenseFile /usr/netscreen/GuiSvc/var/license/license.txt
#guiSvcManager.printLevel debug

Save
```

**NOTE:** If you subsequently change the NSMXpress configuration by using the nsm-setup utility, all manual changes to the configuration files are lost.

### Backing Up the NSM Database

To configure backups of the NSM database, select **NSM Administration > NSM Database Backup** link under NSM Administration. See Figure 19 on page 22.
Figure 19: Database Backup

Database Backup

NSM Backup Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Backup Enabled</td>
<td>o y</td>
</tr>
<tr>
<td>Remote Backup enabled</td>
<td>o n</td>
</tr>
<tr>
<td>Hour of Day to Replicate Database</td>
<td>o 02</td>
</tr>
<tr>
<td>Remote Backup IP</td>
<td></td>
</tr>
</tbody>
</table>

Submit

Execute Backup Now

Apply

Download Database Backup Files

File to Download: /var/netscreen/db_backup/

Download Backups

Changing the NSM Management IP

To change the IP address of the NSM management server, select **NSM Administration > NSM Management IP** link under NSM Administration. See Figure 20 on page 22.

Figure 20: Change Management IP

NSM Management IP

Management Ip: 172.24.66.111

Scheduling Security Updates

To schedule security updates, select **NSM Administration > Schedule Security Updates**. See Figure 21 on page 23.
Figure 21: Schedule Security Updates

Security Update

Select Post Action:
- [ ] update-devices
- [ ] skip

Update Devices after Attack
- Select update device action: Skip/skips update of unconnected device.

User: [ ]
Password: [ ]

Eg: global/super

Schedule Security Updates:
- [ ]

Minutes: [ ]
Hour: [ ]
Day: [ ]
Month: [ ]
Week: [ ]

Run Security Update

Managing System Administration

Use the options in the System Administration section to perform the tasks described in the following sections:

- Rebooting or Shutting Down NSMXpress on page 23
- Changing the User Password on page 24
- Configuring the Network on page 24
- Monitoring with SNMP on page 27
- Forwarding Syslog Messages on page 29
- Changing the System Time on page 33
- Installing Updates on page 34
- Configuring the Web Interface on page 34

Rebooting or Shutting Down NSMXpress

To reboot or shut down NSMXpress, select System Administration > Bootup and Shutdown, and then click either Reboot System or Shutdown System. See Figure 22 on page 23.

Figure 22: Boot Up and Shut Down

Bootup and Shutdown

- Reboot System
- Shutdown System
**Changing the User Password**

To change the user password, select **System Administration > Change User Password**, fill out the form shown in Figure 23 on page 24, and then click **Change**.

![Figure 23: Change User Password](image)

**Configuring the Network**

To access options that allow you to configure the network, select **System Administration > Network Configuration**. The Network Configuration window appears as shown in Figure 24 on page 24.

![Figure 24: Network Interfaces Options](image)

The following sections describe each of the options available in the Network Configuration window:

- Network Interfaces on page 25
- Routing and Gateways on page 25
- Hostname and DNS Clients on page 26
- Host Addresses on page 26
Network Interfaces

Use this option to manage the network interfaces. See Figure 25 on page 25.

Figure 25: Network Interfaces

Routing and Gateways

Use this option to configure and manage routes and gateways. See Figure 26 on page 26.
Figure 26: Routes and Gateways

Routing configuration activated at boot time

<table>
<thead>
<tr>
<th>Default routes</th>
<th>Interface</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>eth0</td>
<td>172.24.88.1</td>
</tr>
</tbody>
</table>

Act as router? (Yes/No)

<table>
<thead>
<tr>
<th>Static routes</th>
<th>Interface</th>
<th>Network</th>
<th>Netmask</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Local routes

<table>
<thead>
<tr>
<th>Interface</th>
<th>Network</th>
<th>Netmask</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Save

Active Routes

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Netmask</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.24.88.0</td>
<td>None</td>
<td>255.255.252.0</td>
<td>eth0</td>
</tr>
<tr>
<td>169.254.0.0</td>
<td>None</td>
<td>255.255.0.0</td>
<td>eth0</td>
</tr>
<tr>
<td>Default Route</td>
<td>172.24.88.1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Hostname and DNS Clients

Use this option to configure and manage hostnames and DNS clients. See Figure 27 on page 26.

Figure 27: DNS Client Options

DNS Client Options

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Resolution order</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSMXpress Juniper.net</td>
<td></td>
</tr>
</tbody>
</table>

Update hostname in host addresses if changed?

<table>
<thead>
<tr>
<th>DNS servers</th>
<th>Search domains</th>
<th>Listed domains</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Host Addresses

Use this option to manage host addresses. See Figure 28 on page 26.

Figure 28: Host Address

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Hostnames</th>
</tr>
</thead>
<tbody>
<tr>
<td>127.0.0.1</td>
<td>NSMXpress Juniper.net, NSMXpress, localhost, localdomain, localhost</td>
</tr>
</tbody>
</table>

Select all. Invert selection. Add a new host address.

Delete Selected Host Addresses
Monitoring with SNMP

You can configure your NSMXpress appliance for SNMP monitoring from a network operations server. The server can then issue periodic SNMP Get instructions to return the status of the NSMXpress appliance.

You configure SNMP on the NSMXpress appliances with access credentials for either SNMP v2c or SNMP v3. NSMXpress supports read-only access to the System Descriptor (sysDescr) and Host Resource MIB.

This section provides instructions for configuring NSMXpress for SNMP monitoring. You must provide access credentials for the SNMP server, a list of IP addresses from which logon requests will be accepted, and the trap conditions to be reported to the SNMP server.

To configure SNMP monitoring of your NSMXpress appliance, select System Administration > SNMP Monitoring. The SNMP window appears. This window contains the tabs described in the following sections:

- SNMP Configuration on page 27
- SNMP System Information on page 28
- SNMP Trap Configuration on page 28

SNMP Configuration

To configure SNMP:

1. Select System Administration > SNMP Monitoring.
2. Select the SNMP Config tab, which is shown in Figure 29 on page 27.

Figure 29: Configuring SNMP

3. Select the version of SNMP to be used, either v2c or v3.
4. Provide authentication information:
   - If you selected SNMP v2c, enter a username.
   - If you selected SNMP v3, enter a username and password.

   The password must be at least 8 characters long.
NSMXpress implements a single username and password, which is effective only for SNMP communication and is not related to any other username and password used on the NSMXpress appliance.

5. To limit SNMP Get requests to specific servers, select Only, and then enter the IP addresses of the permitted servers.

6. Click Save.

**SNMP System Information**

To configure SNMP system information:

1. Select System Administration > SNMP Monitoring.
2. Select the System Info tab, which is shown in Figure 30 on page 28.

**Figure 30: Configuring SNMP System Information**

3. Enter the following information, with is required for any SNMP-managed device:
   - Contact—Contact information for the appliance.
   - Location—Location of the appliance.
   - Description—A brief description of the appliance.
4. Click Save.

**SNMP Trap Configuration**

To configure SNMP trap conditions:

1. Select System Administration > SNMP Monitoring.
2. Select the SNMP Traps tab, which is shown in Figure 31 on page 29.
3. In the Manager IP field, enter the IP address of the SNMP management server.
4. Select from the following trap conditions:
   - **Disk space low**
     Enter the percentage of free disk space below which SNMP issues a trap.
   - **Memory low**
     Enter the percentage of free memory below which SNMP issues a trap.
   - **CPU high**
     Enter the percentage of CPU use over which SNMP issues a trap.
   - **NSM start/stop**
   - **Admin Logon/Logoff**
   - **External IP Unreachable**
     Enter the IP address of the required device.
5. Click **Save**.

**Forwarding Syslog Messages**

NSMXpress provides a simple mechanism for configuring syslog messaging between the NSMXpress appliance and a syslog receiver running rsyslog, syslog-NG, or basic syslog. This mechanism simplifies choosing syslog receivers, data sources of the messages you want to log, and the message transport used.

For the type of message transport, you can choose among TCP, SSL, and UDP. For rsyslog or syslog-NG implementations use TCP or SSL. SSL adds security to TCP, if you select SSL, NSMXpress creates a secure tunnel to the syslog receiver. UDP messaging is available for basic syslog implementations.
The following sections provide procedures for managing syslog message forwarding:

- Viewing Syslog Receivers on page 30
- Adding and Configuring Syslog Receivers on page 31
- Editing Syslog Receiver Configurations on page 33
- Deleting Syslog Receivers on page 33

**Viewing Syslog Receivers**

To view the syslog receivers configured on your NSMXpress appliance, follow these steps:

1. Select **System Administration > Syslog Forwarding**. The Syslog Forwarding window appears. Figure 32 on page 32 shows an example.

2. View the configured syslog receivers in the table in the top portion of the window. Table 3 on page 30 describes the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver</td>
<td>A name provided by the network administrator to identify the syslog receiver</td>
</tr>
</tbody>
</table>
Table 3: Viewing Syslog Receivers (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the syslog receiver</td>
</tr>
<tr>
<td>Type</td>
<td>The protocol used for forwarding messages: UDP, TCP, SSL</td>
</tr>
<tr>
<td>Data sources</td>
<td>The data sources configured for forwarding</td>
</tr>
<tr>
<td>System</td>
<td>The system logs configured to be sent to this receiver.</td>
</tr>
<tr>
<td>Device Server</td>
<td>The Device Server logs configured to be sent to this receiver.</td>
</tr>
<tr>
<td>GUI Server</td>
<td>The GUI Server logs configured to be sent to this receiver.</td>
</tr>
<tr>
<td>HA Server</td>
<td>The HA Server logs configured to be sent to this receiver.</td>
</tr>
</tbody>
</table>

Adding and Configuring Syslog Receivers

To add and configure a syslog receiver, follow these steps:

1. Select **System Administration > Syslog Forwarding**.

2. In the Data Sources section, select the syslog facility for each GUI Server log, Device Server log, and HA Server log. The syslog facility is a field included in the syslog message to help identify the data source.

3. Click **Save**.

4. Click **Add new Receiver**.

   The syslog receiver configuration window appears as shown in Figure 32 on page 32.
5. In the Name field, enter a name for the syslog receiver. This is the name that the syslog receiver will be known by within NSM.

6. In the IP field, Enter the IP address of the syslog receiver.

7. In the Transport field, select the type of syslog receiver:
   - Select **UDP** for basic syslog implementations.
   - Select **TCP** for rsyslog or syslog-NG implementations.
Select SSL to create a secure tunnel to a syslog receiver in rsyslog or syslog-NG implementations.

In the System Logs section of the Data Sources table, select the sources of data from which system messages will be forwarded to the syslog receiver. These sources can include NSMxpress system messages, package updates, and mail logs.

In the NSM section of the Data Sources table, select each GUI Server log, Device Server log, and HA Server log to be forwarded to the syslog receiver.

8. Click Save to save and apply the configuration.

**Editing Syslog Receiver Configurations**

To edit a syslog receiver configuration, follow these steps:

1. Select **System Administration > Syslog Forwarding**.
2. In the Syslog Receivers window, click the name of the syslog receiver you want to edit.

   The syslog receiver configuration window appears for the selected receiver.

3. Make the desired changes to the configuration.
4. Click **Save** to save and apply your edits to the configuration of this syslog receiver.

**Deleting Syslog Receivers**

To delete a syslog receiver configuration, follow these steps:

1. Select **System Administration > Syslog Forwarding**.
2. In the Syslog Receivers window, check the box next to each syslog receiver you want to delete.
3. Click **Delete selected receivers**.

   NSMxpress deletes the selected syslog receivers and any secure tunnels configured for their use.

**Changing the System Time**

To set the system time, select **System Administration > System Time**. From the System Time window, you can perform the following functions:

- Set or change the system time.
- Set the time zone.
- Configure an NTP server to synchronize the system time with an external clock.
Installing Updates

Select **System Administration > System Update** to perform the following tasks:

- Check for updates and install them.
- Enable or disable automatic updates.
- Install a new NSMXpress version.
- Add or modify proxy settings for the Yum server.

Configuring the Web Interface

To specify which NSM client computers can access NSMXpress through the Web interface, select **System Administration > WebUI Configuration**. The Allowed IP Addresses window appears as shown in Figure 33 on page 34.

![Figure 33: Web Interface Access](image)

Maintaining NSMXpress

The Maintaining section of the NSMXpress navigation tree allows you to perform the tasks described in the following sections:

- Viewing System Statistics on page 34

Viewing System Statistics

To view system statistics, select **System Administration > Maintenance > System Statistics**. The system Statistics window appears as shown in Figure 34 on page 35.
**System Statistics**

**CPU**
Select CPU to view graphs that monitor the CPU activity hourly, daily, weekly, monthly, or on a customizable basis.

**Log Rate**
Select lograte to view graphs that monitor the log rate hourly, daily, weekly, monthly, or on a customizable basis.

**CPU Load**
Select Load to view graphs that monitor the CPU load hourly, daily, weekly, monthly, or on a customizable basis.

**Memory Data**
Select Memory to view graphs that monitor the memory activity hourly, daily, weekly, and monthly.

**Network Data**
Select either eth0 or eth1 to view graphs that monitor network activity hourly, daily, weekly, and monthly.

**Process Count**
Select Process to view graphs that monitor the number of processes hourly, daily, weekly, and monthly.

**Disk Data**
Select Disk to view graphs that monitor the file system disk space usage hourly, daily, weekly, and monthly.
Tile All Graphs

Select Tile all graphs to display all the statistical graphs for the system in one window.

Troubleshooting

Use the options in the Troubleshooting section to access the following information and utilities:

- Error Logs on page 36
- Network Utilities on page 37
- Tech Support on page 39

Error Logs

To review error logs, select Troubleshooting > Error Logs. Figure 35 on page 36 shows an example.

Figure 35: Review Error Logs

<table>
<thead>
<tr>
<th>Log File</th>
<th>Description</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>File /ns/screen/DevSw/screenLog/deviceDaemon.0</td>
<td>Device Server Error Log</td>
<td>View</td>
</tr>
<tr>
<td>File /ns/screen/DevSw/screenLog/pro.cc.log</td>
<td>Data Collector Error Log</td>
<td>View</td>
</tr>
<tr>
<td>File /ns/screen/DevSw/screenLog/gproDDM.log</td>
<td>Device Directive Manager Error Log</td>
<td>View</td>
</tr>
<tr>
<td>File /ns/screen/DevSw/screenLog/newLogWalker.0</td>
<td>NewLog Walker Error Log</td>
<td>View</td>
</tr>
<tr>
<td>File /ns/screen/DevSw/screenLog/profilerManager.0</td>
<td>Profiler Manager Error Log</td>
<td>View</td>
</tr>
<tr>
<td>File /ns/screen/DevSw/screenLog/statusMonitor.0</td>
<td>Status Monitor</td>
<td>View</td>
</tr>
<tr>
<td>File /ns/screen/GuiSw/serverErrorLog/guiDaemon.0</td>
<td>Gui Server Error Log</td>
<td>View</td>
</tr>
<tr>
<td>File /ns/screen/GuiSw/serverErrorLog/guiController.0</td>
<td>Gui Controller Error Log</td>
<td>View</td>
</tr>
<tr>
<td>File /ns/screen/GuiSw/serverErrorLog/gproDDM.log</td>
<td>Gui Directive Manager Error Log</td>
<td>View</td>
</tr>
<tr>
<td>File /ns/screen/GuiSw/serverErrorLog/statusMonitor.0</td>
<td>GuiSw Status Monitor Error Log</td>
<td>View</td>
</tr>
<tr>
<td>File /ns/screen/HalSw/serverErrorLog/highAvail.0</td>
<td>High Avail Error Log</td>
<td>View</td>
</tr>
</tbody>
</table>

To view details of an individual error log, select the file you want to view and click View. Figure 36 on page 36 shows sample error log details.

Figure 36: Error Log Detail
Network Utilities

To access basic network utilities (ping, traceroute, and nslookup) for TCP/IP Networking, select Troubleshooting > Network Utilities. These tools also provide an IP subnet calculator. See Figure 37 on page 37.

Figure 37: Network Utilities Options

Ping

Ping is a tool for checking network connectivity. NSMXpress prompts with questions so you can focus your search.

Figure 38 on page 37 shows an example.

Figure 38: Ping Utility

Hostname

How many Packets?

Packet Size?

Pattern(s) to send (Hex)?

How many sec between sending each packet?

Pattern(s) to send (Hex)?

How Many Packets

Enter the number of packets this ping command will send. The default is 5. The values range from 1-99.

Packet Size

Enter the packet size (in bytes) this ping command will send. The default is 56. The values range from 1-9999.

How Many Sec Between Sending Each Packet

Enter how much time (in seconds) ping should wait between sending each packet.
Patterns to Send (Hex)

The data sent by ping contains a hexadecimal pattern. If you leave this option blank, ping will fill it with random data. This option is useful if you do not have problems with connectivity itself but with data loss.

Verbosity Output

NSMXpress lists the ICMP packets (other than ECHO_Response) that have been received.

Numeric Output Only

Check this option if you do not want any attempts to be made to look up symbolic names for host addresses.

Bypass Routing Tables

If the host is not a directly attached network, an error is returned. This option can be used to ping a local host through an interface that has no route through it.

Traceroute

Traceroute is a tool to print the route a packet takes to a network host. See Figure 39 on page 38.

Figure 39: Traceroute Utility

NOTE: The only required field is Hostname. The value can be either a hostname or an IP address.
Lookup

Use the lookup tool to obtain the IP address from a hostname and the hostname from an IP address (see Figure 40 on page 39). The query type drop-down list contains several types of records found in the DNS database. Enter a nameserver or select the default. If you choose the default, nslookup will use the server on which NSMXpress is installed.

Figure 40: Lookup Utility

IP Subnet Calculator

Use the IP subnet calculator to calculate the netmask for a TCP/IP-network. You can calculate a netmask by class and subnet bits or by the number of hosts (see Figure 41 on page 39). When you calculate a netmask by the number of hosts, NSMXpress returns the smallest network available.

Figure 41: IP Subnet Calculator

Tech Support

To get contact information for Juniper Networks technical support, select Troubleshooting > Tech Support under Troubleshooting. To help analyze problems, select a detail type in the drop-down list box, and then click Run Tech-Support Script. NSMXpress creates a file you can download and send to Juniper Networks technical support. See Figure 42 on page 40.
Figure 42: Juniper Tech Support

Tech Support

Details from GUI, Device and HA servers

Run Tech-Support Script

JTAC WEBSITE: https://support.juniper.net

JTAC PHONE NUMBER: 1-800-314-JTAC

JTAC FTP SITE: ftp.juniper.net

Viewing System Information

Use the System Information menu item to display information about the server, including CPU load and memory use, as shown in Figure 43 on page 40.

Figure 43: System Information

| System hostname: NSMXpress juniper.net |
| Operating system: Juniper NSMXpress 2003.1r1 |
| Server Uptime: 0 days, 27 |
| CPU load averages: 0.00 (1 min) 0.02 (5 mins) 0.01 (15 mins) |
| Real memory: 3.96 GB total, 108 MB used |
| Virtual memory: 7.81 GB total, 0 bytes used |

List of Technical Publications

Table 4 on page 41 describes the documentation for NSMXpress and NSM.
### Table 4: Network and Security Manager Publications

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

### 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.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at http://www.juniper.net/customers/support/downloads/710059.pdf.
Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.

JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

Revision History

December 22, 2008—530-028103-02 Revision 1.

Copyright © 2008, 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. JUNOSe 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, 6,538,999, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.