

# Network and Security Manager NSM3000

## Quick Start

May 18, 2010.2  
Revision 1

NSM3000 is an appliance version of Network and Security Manager (NSM). NSM3000 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 NSM3000 because it eliminates the need to have dedicated resources for maintaining a network and security management solution.

NSM3000 makes it easy for administrators to control device configuration, network settings, and security policy settings for multiple families of Juniper devices including:

- IDP Series Intrusion Detection and Prevention Appliances and Firewall and VPN devices running ScreenOS.
- Devices running JUNOS software, such as J Series Services Routers, SRX Series Services Gateways, EX Series Ethernet Switches, M Series Multiservice Edge Routers, and MX Series Ethernet Services routers.
- SA Series SSL VPN Appliances
- IC Series Unified Access Control Appliances

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 NSM3000 concurrently.

This quick start explains the following steps for installing and configuring NSM3000 and for configuring NSM.

1. Install the NSM3000 appliance hardware.
2. Set up the NSM3000 appliance, using the serial port.

3. Configure the NSM software, using the Web interface.
4. Configure the NSM software, which is preinstalled onto the NSM3000 appliance, with site-specific parameters.

## Contents

Hardware Installation . . . . .	4
NSM3000 Ports . . . . .	4
Installing the NSM3000 Hardware . . . . .	5
Initial Setup Configuration . . . . .	7
Boot NSM3000 . . . . .	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 the Statistical Report Server (SRS) (Regional Server Only) . . . . .	16
Installing NSM Software . . . . .	17
Managing NSM Administration . . . . .	17
Changing the Superuser Password . . . . .	17
Downloading NSM MIBS (Regional Server Only) . . . . .	18
Exporting Audit Logs . . . . .	18
Exporting Device Logs (Regional Server Only) . . . . .	18
Generating Reports (Regional Server Only) . . . . .	19
Modifying NSM Configuration Files . . . . .	19
Backing Up the NSM Database . . . . .	20
Changing the NSM Management IP . . . . .	21
Scheduling Security Updates . . . . .	21
Managing System Administration . . . . .	22
Rebooting or Shutting Down NSM3000 . . . . .	22
Changing the User Password . . . . .	23
Configuring the Network . . . . .	23
Network Interfaces . . . . .	23
Routing and Gateways . . . . .	24
Hostname and DNS Clients . . . . .	24
Host Addresses . . . . .	25
Managing RADIUS Servers . . . . .	25
Adding a RADIUS Server . . . . .	26
Changing the Priority of RADIUS Servers . . . . .	27
Deleting a RADIUS Server . . . . .	27
Editing RADIUS Server Parameters . . . . .	27
Monitoring with SNMP . . . . .	28
SNMP Configuration . . . . .	28
SNMP System Information . . . . .	29
SNMP Trap Configuration . . . . .	30

---

Forwarding Syslog Messages .....	31
Viewing Syslog Receivers .....	31
Adding and Configuring Syslog Receivers .....	32
Editing Syslog Receiver Configurations .....	34
Deleting Syslog Receivers .....	34
Changing the System Time .....	34
Installing Updates .....	34
Managing Users .....	35
Creating New NSM3000 Users .....	35
Deleting a User .....	37
Editing User Attributes .....	37
Understanding User Profiles .....	37
Configuring the Web Interface .....	39
Maintaining NSM3000 .....	39
Viewing System Statistics .....	39
CPU .....	40
Log Rate .....	40
CPU Load .....	40
Memory Data .....	40
Network Data .....	40
Process Count .....	40
Disk Data .....	40
Tile All Graphs .....	40
Upgrading the Recovery Partition .....	40
Troubleshooting .....	42
Auditing User Operations .....	42
Error Logs .....	44
Network Utilities .....	44
Ping .....	44
Traceroute .....	45
Lookup .....	46
IP Subnet Calculator .....	46
Tech Support .....	47
Viewing System Information .....	47
List of Technical Publications .....	48
Requesting Technical Support .....	49
Self-Help Online Tools and Resources .....	49
Opening a Case with JTAC .....	50
Revision History .....	50

## Hardware Installation

We recommend that you install NSM3000 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 NSM3000 in your DMZ, ensure that it can connect to your internal resources.

## NSM3000 Ports

Table 1 on page 4 provides required port information on the NSM3000.

**Table 1: Required Ports on NSM3000**

Direction	Port	Description	LAN	Internet	Depends on Configuration
In	22	SSH command-line management	Yes	No	No
	443	Web interface for administrator login	Yes	No	No
	8443	Web interface for listening for NSM API messages.	LAN	Yes	Yes
	7800	Connections from managed devices to NSM3000	Yes	Yes	No
	7801	Connections from the NSM GUI Client to NSM	Yes	No	No
	7802	Heartbeat between peers in an HA cluster	Yes	No	Yes
	7803	Connections from managed IDP devices to NSM	Yes	Yes	Yes
	7804	Connections from devices running JUNOS, Secure Access devices, or Infranet Controller devices	Yes	Yes	Yes

Table 1: Required Ports on NSM3000 (continued)

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

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

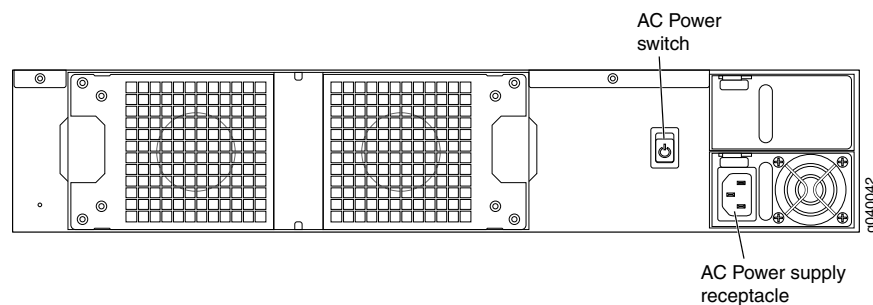
## Installing the NSM3000 Hardware

Follow these steps to unpack the NSM3000 appliance and connect it to your network.

To install NSM3000:

1. Place the shipping container on a flat surface and remove the hardware components with care.
2. Remove the NSM3000 device from the shipping container and place it on a flat surface.
3. Mount NSM3000 in your server rack using the attached mounting brackets.
4. Plug the power cord into the AC receptacle on the rear panel.

Figure 1: Rear Panel of NSM3000



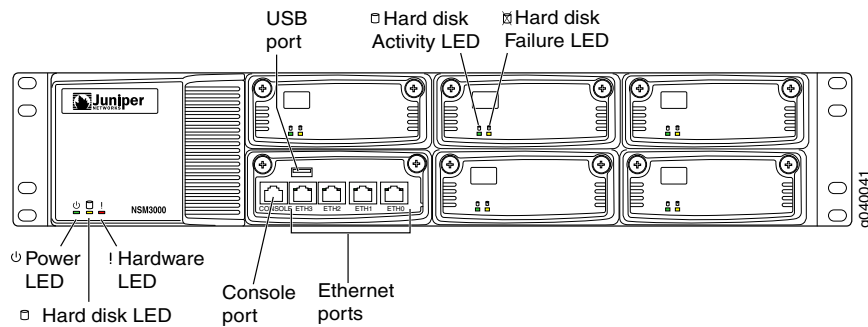
If your NSM3000 contains two power supplies, plug a power cord into each AC receptacle.

5. Plug the other end of the power cord into a wall socket.

If your NSM3000 contains two power supplies, plug each power cord into a separate power circuit to ensure that the NSM3000 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.

**Figure 2: Front Panel of NSM3000**



7. Plug the null modem serial cable into the console port.

This cable was shipped with your NSM3000. 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 NSM3000 hard disk LED turns on whenever the appliance reads data from or writes data to an NSM3000 hard disk.

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

Table 2 on page 6 provides LED information for the Ethernet ports.

**Table 2: Ethernet Port LEDs**

LAN Status	LED 1	LED2
10 Mbps connection	Off	Off
100 Mbps connection	Green	Off
1000 Mbps connection	Orange	Off
Data is being transferred	Orange, Green, or Off	Blinking
No connection	Off	Off

---

## Initial Setup Configuration

---

When you first turn on an unconfigured NSM3000 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 NSM3000 for the first time:

- Boot NSM3000 on page 7
- Set Up Your Appliance on page 7

### Boot NSM3000

To configure NSM3000 for the first time, you must attach your NSM3000 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 NSM3000 console port.
3. Turn on the NSM3000 appliance.

When NSM3000 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.

```
NSM3press.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 Netfileter 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/administration
```

```
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.
```

```
[admin@NSMXpress ~]$
```

To configure the NSM software using the CLI, see the *NSMXpress and NSM3000 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 the NSM3000:

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

2. Open a Web browser and paste the URL into the address text box.
3. Press Enter to open the NSM appliance 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 NSM3000 appliance from the Web interface.

---

## Configuring the NSM Software

After you log 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 NSM3000 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 NSM3000 Web interface, NSM3000 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 NSM3000 hardware as described in “Hardware Installation” on page 4.
2. Boot and setup your NSM3000 appliance as described in “Initial Setup Configuration” on page 7.
3. Enter the **https://<ip>/administration** URL for your appliance in a Web browser. See “Web Interface Configuration” on page 8 for details.
4. Log into the Web interface. The **System Info** page opens.
5. Click the link **Install NSM Regional Server** (see Figure 3 on page 10) to go to the Install Regional Server window or click the **Install NSM Central Manager** link to view the Install NSM Central Manager window (see Figure 4 on page 10), as the case may be.



NOTE: The “admin” user default username is *admin* and the password is the one you created in Step 6 of “Boot NSM3000” on page 7.

Figure 3: Regional Server Configuration Main Menu

Login: admin

- » NSM Administration
  - » Install NSM Regional Server
  - » System Administration
  - » Maintenance
  - » Troubleshooting
- » System Information
- » Logout

## Install NSM Regional Server

**NSM Configuration Main Menu**

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

**NSM 'super' password**   
 Password for 'super' user

**NSM License type**  Base Install  Upload license file:  
 Specify a license file, or select "Base Install" to use the built-in limited device license.

**Remote Replication of Database** Off [Menu](#)

**High Availability** Off [Menu](#)

**SRS** Off [Menu](#)

Figure 4: Central Manager Configuration Main Menu

Login: admin

- » NSM Administration
  - » Install NSM Central Manager
  - » System Administration
  - » Maintenance
  - » Troubleshooting
- » System Information
- » Logout

## Install NSM Central Manager

**NSM Configuration Main Menu**

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

**NSM 'super' password**   
 Password for 'super' user

**Remote Replication of Database** Off [Menu](#)

**High Availability** Off [Menu](#)

6. 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.

7. 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.

8. 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.

9. 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.

10. 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 5 on page 12.

**Figure 5: High Availability Options**

The screenshot shows the 'Menu: High Availability' configuration page. It includes several settings:

- High Availability:** A dropdown menu with 'n' selected, indicating HA is currently off. Below it is the text 'Whether to enable HA on this server or not'.
- Primary Status:** A dropdown menu with 'y' selected, indicating the server is the primary. Below it is the text 'If 'y', this machine is a Primary Server and if 'n' this machine is a Secondary Server'.
- HA Remote IP:** An empty text input field with the description 'IP address for the peer's primary heartbeat link'.
- HA Link Failure Detection IP:** An empty text input field with the description 'IP address outside the HA cluster'.
- HA Inter-server password:** Two empty text input fields with the description 'Shared password for heartbeat'.
- Shared Disk:** A toggle set to 'Off' with a 'Menu' link next to it.
- HA Links:** A 'Menu' link.
- HA Advanced Settings:** A 'Menu' link.

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 NSM3000 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 5 on page 12) to configure a shared disk for regional servers (see Figure 6 on page 13) or for central managers (see Figure 7 on page 13.) This step is optional.

Figure 6: Shared Disk Options for Regional Servers

Menu: Shared Disk	
<b>Shared Disk: Gui Server</b>	<input checked="" type="radio"/> n <input type="radio"/> c <input type="text" value="y"/>
If 'y', data directory for GUI Server is a shared disk partition	
<b>Shared Disk: Device Server</b>	<input checked="" type="radio"/> n <input type="radio"/> c <input type="text" value="y"/>
If 'y', data directory for Device Server is a shared disk partition	
<b>Shared Disk Source (NFS)</b>	<input type="text"/>
Source of shared disk, e.g. /dev/sdc1 or server:/share	
<b>Shared Disk NFS Mount Options</b>	<input checked="" type="radio"/> rw <input type="radio"/> c <input type="text"/>
Options when mounting shared disk e.g. rw,intr,tcp,soft,timeo	

Figure 7: Shared Disk Options for Central Managers

Menu: Shared Disk	
<b>Shared Disk: Gui Server</b>	<input type="text" value="y"/>
If 'y', data directory for GUI Server is a shared disk partition	
<b>Shared Disk Source (NFS)</b>	<input type="text"/>
Source of shared disk, e.g. /dev/sdc1 or server:/share	
<b>Shared Disk NFS Mount Options</b>	<input type="text"/>
Options when mounting shared disk e.g. rw,intr,tcp,soft,timeo	

NSM3000 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*.

- Click **Menu** next to HA Links (see Figure 5 on page 12) to configure the second link in the HA cluster (see Figure 8 on page 13). This step is optional.

Figure 8: HA Links Options

Menu: HA Links	
<b>HA Link count</b>	<input checked="" type="radio"/> 1 <input type="radio"/> c <input type="text" value="1"/>
Number of heartbeat links between the Primary and Secondary Servers.	

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 23 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 9: Redundant Links

Menu: HA Links	
<b>HA Link count</b>	<input checked="" type="radio"/> 2 <input type="radio"/> 1
Number of heartbeat links between the Primary and Secondary Servers.	
<b>HA Link 2 Local IP</b>	<input type="text"/>
IP address for this machine's secondary heartbeat link	
<b>HA Link 2 Remote IP</b>	<input type="text"/>
IP address for the peer's secondary heartbeat link	
<b>HA Remote Replication IP</b>	<input type="text"/>
IP address used for remote HA replications	

- Click **Menu** next to HA Advanced Settings (see Figure 5 on page 12) to configure HA Advanced settings (see Figure 10 on page 14). This step is optional.

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

Figure 10: HA Advanced Settings

Menu: HA Advanced Settings	
<b>HA Heartbeat Frequency</b>	<input checked="" type="radio"/> 15 <input type="radio"/> <input type="text"/>
Time interval in seconds between heartbeat messages (Default is 15 seconds) (Range is 5 to 3600)	
<b>HA Heartbeat Failure Threshold</b>	<input checked="" type="radio"/> 4 <input type="radio"/> <input type="text"/>
Number of missing heartbeat messages before automatic switchover occurs (Default is 4 missing messages) (Range is 1 to 10000)	
<b>HA Data Replication Timeout</b>	<input checked="" type="radio"/> 1800 <input type="radio"/> <input type="text"/>
Rsync Command Replication Timeout (Default is 1800 seconds) (Range is 1 to 65535)	

- 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 11 on page 14.

Figure 11: Advanced Options Menu

Menu: Advanced Options	
<b>https port for NBI service</b>	<input checked="" type="radio"/> 8443 <input type="radio"/> <input type="text"/>
The port number to listen for NBI (Default is 8443)	
<b>Remote Replication of Database SRS</b>	Off <input type="radio"/> <a href="#">Menu</a>
	Off <input type="radio"/> <a href="#">Menu</a>

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 NSM3000 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 the Statistical Report Server (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 5 on page 12) to configure daily backups (see Figure 12 on page 15).

**Figure 12: Remote Replication of Database Options**

Menu: Remote Replication of Database	
<b>Remote Replication of Database</b>	<input type="radio"/> n <input checked="" type="radio"/> y
If 'y', local backups will be sent to a remote backup machine	
<b>Hour of day to Replicate Database</b>	<input type="radio"/> 02 <input type="radio"/> 00
Hour to start a backup	
<b>Remote Backup IP</b>	<input type="text"/>
IP address of a remote backup machine	
<b>Remote Replication Timeout (seconds)</b>	<input type="radio"/> 1800 <input type="text"/>
Rsync Command Backup Timeout (seconds) (Default is 1800 seconds) (Range is 1 to 65535)	

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 through 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 through 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 the Statistical Report Server (SRS) (Regional Server Only)

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

1. On the Advanced Options menu, click **Menu** next to SRS (see Figure 5 on page 12) to open the SRS menu (see Figure 13 on page 16).

Figure 13: SRS Menu

Menu: SRS		
<b>SRS</b>	<input checked="" type="radio"/> n	<input type="radio"/> y
Statistical Report Server will be used with this GUI Server		
<b>SRS DB IP</b>		<input type="text"/>
Database server IP address		
<b>SRS DB Type</b>	<input checked="" type="radio"/> pgsql	<input type="radio"/> pgsql
Database type		
<b>SRS Database Name</b>	<input checked="" type="radio"/> netscreen	<input type="text"/>
Database name		
<b>SRS DB Owner Name</b>	<input checked="" type="radio"/> netscreen	<input type="text"/>
Database user name		
<b>SRS DB Owner Password</b>		<input type="text"/>
Database password		

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 the password 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 NSM3000 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.

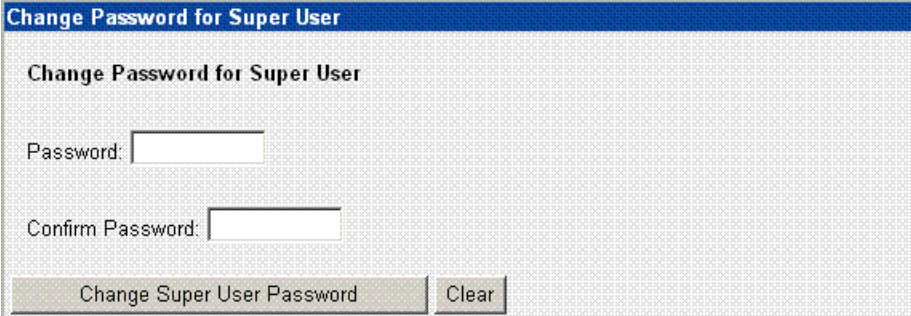
The following sections explain how to use each of the NSM Administration options:

- Changing the Superuser Password on page 17
- Downloading NSM MIBS (Regional Server Only) on page 18
- Exporting Audit Logs on page 18
- Exporting Device Logs (Regional Server Only) on page 18
- Generating Reports (Regional Server Only) on page 19
- Modifying NSM Configuration Files on page 19
- Backing Up the NSM Database on page 20
- Changing the NSM Management IP on page 21
- Scheduling Security Updates on page 21

## Changing the Superuser Password

To change the superuser password, select **NSM Administration > NSM Super User Password**. See Figure 14 on page 17.

Figure 14: Change Superuser Password



**Change Password for Super User**

**Change Password for Super User**

Password:

Confirm Password:

## Downloading NSM MIBS (Regional Server Only)

To download any available MIBs, select **NSM Administration > Download NSM MIBS**, and then click **Download MIB**. See Figure 15 on page 18. This option is not available on the central manager.

Figure 15: Download NSM MIBs



## Exporting Audit Logs

To export audit logs, select **NSM Administration > Export Audit Logs**. See Figure 16 on page 18.

Figure 16: Export Audit Logs



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 system log 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 17 on page 18). This option is not available on the central manager.

Figure 17: Export Device Logs



## Generating Reports (Regional Server Only)

To generate reports, select **NSM Administration > Generate Reports**. See Figure 18 on page 19. This option is not available on the central manager.

Figure 18: Generate Reports

**Generate Reports**

The Reports need to be created by logging in through the UI, before running the script below.

Domain:  Type:  Report:  Script:   
 Eg: global Eg: system/shared Eg: mytest Eg: ftp.sh/email.sh

User:  Password:   
 Eg: global/super

Schedule Reports:

Minutes:  Hour:  Day:  Month:  Week Day:



**NOTE:** The user is an NSM administrator and not an NSM3000 user. Enter a user name as *domain/user*, such as *global/super*.

## Modifying NSM Configuration Files

To manually edit the `GuiSrv.cfg`, `DevSvr.dfg` and `HaSvr.cfg` files, select **NSM Administration > Modify NSM Configuration Files**. The example in Figure 19 on page 20 shows the option to modify the `GuiSrv.cfg` file.

Figure 19: NSM Configuration Files

## NSM Configuration Files

**GuiSvr.cfg** [DevSvr.cfg](#) [HaSvr.cfg](#)

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

**The server will be restarted once the changes are made.**

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

setuid.user          nsm
clientId             0
peerGuiSvrId        2
clientOneTimePassword dk2003ns

default.printLevel   warn
default.printProperties where=file, sync=0, maxfilenum=25
#statusMonitor.printLevel debug
#statusMonitor.printProperties where=file, sync=1, maxfilenum=250
#guiSvrDirectiveHandler.printLevel debug
#guiSvrLicenseManager.printLevel debug
#guiSvrMasterController debug
guiSvrLicenseManager.licenseFile /usr/netscreen/GuiSvr/var/license/license.txt
#guiSvrManager.printLevel debug
```

Save



**NOTE:** If you subsequently change the NSM3000 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 20 on page 21.

Figure 20: Database Backup

## Database Backup

NSM Backup Configuration Parameters			
Local Backup Enabled	<input checked="" type="radio"/> y	<input type="radio"/>	<input type="text" value="y"/>
Remote Backup enabled	<input checked="" type="radio"/> n	<input type="radio"/>	<input type="text" value="y"/>
Hour of Day to Replicate Database	<input checked="" type="radio"/> 02	<input type="radio"/>	<input type="text" value="00"/>
Remote Backup IP	<input type="text"/>		
<input type="button" value="Submit"/>			
Execute Backup Now			
<input type="button" value="Apply"/>			
Download Database Backup Files			
File to Download	<input type="text" value="/var/netscreen/dbbackup/"/> <input type="button" value="..."/>		
<input type="button" value="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 21 on page 21.

Figure 21: Change Management IP

NSM Management IP	
Management Ip	<input checked="" type="radio"/> 172.24.68.111 <input type="radio"/> <input type="text"/>

### Scheduling Security Updates

To schedule security updates, select **NSM Administration > Schedule Security Updates**. See Figure 22 on page 22.

Figure 22: 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: Day: Week

Run Security Update

## Managing System Administration

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

- Rebooting or Shutting Down NSM3000 on page 22
- Changing the User Password on page 23
- Configuring the Network on page 23
- Managing RADIUS Servers on page 25
- Monitoring with SNMP on page 28
- Forwarding Syslog Messages on page 31
- Changing the System Time on page 34
- Installing Updates on page 34
- Managing Users on page 35
- Configuring the Web Interface on page 39

### Rebooting or Shutting Down NSM3000

To reboot or shut down NSM3000, select **System Administration > Bootup and Shutdown**, and then click either **Reboot System** or **Shutdown System**. See Figure 23 on page 22.

Figure 23: Reboot or 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 24 on page 23, and then click **Change**.

Figure 24: Change User Password

**Changing NSMXpress user password**

Changing password for admin

Old password

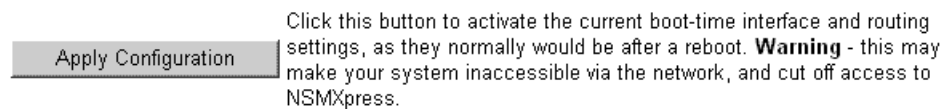
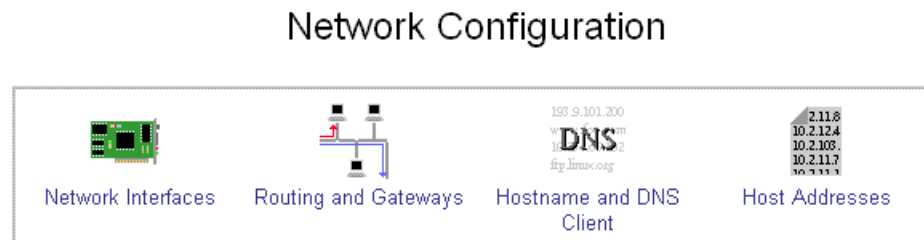
New password

New password (again)

## 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 25 on page 23.

Figure 25: Network Interfaces Options



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

- Network Interfaces on page 23
- Routing and Gateways on page 24
- Hostname and DNS Clients on page 24
- Host Addresses on page 25

### Network Interfaces

Use this option to manage the network interfaces. See Figure 26 on page 24.

Figure 26: Network Interfaces

Module Index

## Network Interfaces

## Interfaces Active Now

Select all. | Invert selection. | Add a new interface.

	Name	Type	IP Address	Netmask	Status
<input type="checkbox"/>	eth0	Ethernet	172.24.68.111	255.255.252.0	Up
<input type="checkbox"/>	lo	Loopback	127.0.0.1	255.0.0.0	Up

Select all. | Invert selection. | Add a new interface.

De-Activate Selected Interfaces

## Interfaces Activated at Boot Time

Select all. | Invert selection. | Add a new interface. | Add a new address range.

	Name	Type	IP Address	Netmask	Activate at boot?
<input type="checkbox"/>	eth0	Ethernet	172.24.68.111	255.255.252.0	Yes
<input type="checkbox"/>	eth1	Ethernet	From DHCP	Automatic	No
<input type="checkbox"/>	lo	Loopback	127.0.0.1	255.0.0.0	Yes

Select all. | Invert selection. | Add a new interface. | Add a new address range.

Delete Selected Interfaces

Delete and Apply Selected Interfaces

Apply Selected Interfaces

## Routing and Gateways

Use this option to configure and manage routes and gateways. See Figure 27 on page 24.

Figure 27: Routes and Gateways

**Routing configuration activated at boot time**

**Default routes**

Interface	Gateway
eth0	172.24.68.1

Act as router?  Yes  No

**Static routes**

Interface	Network	Netmask	Gateway

**Local routes**

Interface	Network	Netmask

Save

## Active Routes

	Destination	Gateway	Netmask	Interface
<input type="checkbox"/>	172.24.68.0	None	255.255.252.0	eth0
<input type="checkbox"/>	169.254.0.0	None	255.255.0.0	eth0
<input type="checkbox"/>	Default Route	172.24.68.1		eth0

## Hostname and DNS Clients

Use this option to configure and manage hostnames and DNS clients. See Figure 28 on page 25.

Figure 28: DNS Client Options

Host Addresses

Use this option to manage host addresses, See Figure 29 on page 25.

Figure 29: Host Address

IP Address	Hostnames
<input type="checkbox"/> 127.0.0.1	NSMXpress.juniper.net , NSMXpress , localhost.localdomain , localhost

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

Delete Selected Host Addresses

Managing RADIUS Servers

The NSM3000 WebUI supports authentication of users defined in the RADIUS servers, in addition to authentication of locally defined admin users.

When a user logs into NSM3000 using the WebUI, the software first checks the UNIX user database and then the WebUI user database to authenticate the user. If the user is not a locally defined admin user, the software contacts the RADIUS servers added to the RADIUS server list in the Web UI to authenticate the user. The RADIUS servers are contacted in the order of priority set in the RADIUS server list. If any of the RADIUS servers authenticates the user, the user is logged in with the privileges that are associated with the user profile. If none of the servers authenticates the user, the user login fails.



NOTE: The NSM3000 appliance must be configured as a RADIUS client on a RADIUS server so that the RADIUS server responds to authentication requests from NSM3000. Select any Juniper Make or Model in the Make/Model field while adding an NSM3000 appliance as a RADIUS client. You will need to update the juniper dictionary file (juniper.dct) in the RADIUS server with the Juniper defined Vendor-Specific Attribute (VSA) for NSM3000:ATTRIBUTE Juniper-Nsmxpress-Profile Juniper-VSA(6, string) r. You will also need to add NSM3000 users with their associated user profiles (SysAdmin, NSMAdmin, Operator, Guest), to the RADIUS database. For more details see *Steel-Belted Radius Documentation*.



NOTE: You need System Administration or NSM Administration permission to manage RADIUS servers in the NSM3000 WebUI.

The following sections explain how to manager a RADIUS server:

- Adding a RADIUS Server on page 26
- Changing the Priority of RADIUS Servers on page 27
- Deleting a RADIUS Server on page 27
- Editing RADIUS Server Parameters on page 27

### Adding a RADIUS Server

To add a RADIUS server:

1. Select **System Administration > Radius Management**. The RADIUS Servers dialog box appears listing the RADIUS Servers that have been added. See Figure 30 on page 26.

Figure 30: RADIUS Servers Dialog Box

Radius Servers

RADIUS Servers							
	Name	Host	Auth Port	Accounting Port	COA Port	Retries	Timeout
<input type="checkbox"/>	RadiusSvr2	10.204.77.118	1812	1813	4600	1	3
<input type="checkbox"/>	RadiusSvr1	jghosh-dc.jnpr.net	1812	1813	4564	1	3

Add Delete Selected Move Up Move Down Select All

2. Click **Add** to add a RADIUS Server to the WebUI. The Add Radius Server dialog box appears. See Figure 31 on page 26.

Figure 31: Add RADIUS Server Dialog Box

Add Radius Server

Add RADIUS Server

Name	server1
Server address	10.206.144.154
Shared secret	••••••••
Auth port	1645
Acct port	1646
Disconnect/CoA port	1700
Timeout(secs)	3
Retries	1

Add Clear

← Return to Radius Servers list

3. Configure the following parameters in the Add RADIUS Server dialog box:
  - a. **Name:** The name of the user to be authenticated by the RADIUS server.
  - b. **Server address:** The IP address or the hostname of the RADIUS Server.
  - c. **Shared secret:** The shared secret NSM3000 and the RADIUS server use for secure authentication.
  - d. **Auth Port:** The RADIUS authentication software port. (We recommend UDP port 1812)

- e. **Acct Port:** The RADIUS accounting software port. (We recommend UDP port 1813)
  - f. **Disconnect/CoA port:** The change of authorization or disconnect port.
  - g. **Timeout (sec):** Automatic time out in second(s) of the RADIUS access-request after which the request will be retransmitted, if applicable. Enter a value between 1 and 10 seconds.
  - h. **Retries:** The number of times the RADIUS access-request must be retransmitted for RADIUS authentication. Enter a value between 1 and 5.
4. Click **Add**. The RADIUS Servers dialog box appears with the RADIUS Server you added listed.

### Changing the Priority of RADIUS Servers

To change the priority of RADIUS servers:

1. Select **System Administration > Radius Management**. The RADIUS Servers dialog box appears listing the RADIUS Servers that have been added.
2. To increase the priority of a RADIUS server, select the check box next to the name of the server whose priority you want to increase, and click **Move Up**.

To decrease the priority of a RADIUS server, select the check box next to the name of the server whose priority you want to decrease, and click **Move Down**.

### Deleting a RADIUS Server

To delete a RADIUS server:

1. Select **System Administration > Radius Management**. The RADIUS Servers dialog box appears listing the RADIUS Servers that have been added.
2. Select the check box next to the name of the server you want to delete, and click **Delete Selected**.



NOTE: You need **System Administration** permissions to delete RADIUS servers.

### Editing RADIUS Server Parameters

To edit the parameters of a RADIUS server:

1. Select **System Administration > Radius Management**. The RADIUS Servers dialog box appears listing the RADIUS Servers that have been added.
2. Select the name of the server whose properties you want to edit. The Edit RADIUS Server dialog box appears. See Figure 32 on page 28.

Figure 32: Edit RADIUS Server Dialog Box

Module Index Edit Radius Server

---

Edit Radius Server	
Name	server1
Server address	10.206.144.154
Shared secret	••••••
Auth port	1645
Acct port	1646
Disconnect/CoA port	1700
Timeout(secs)	3
Retries	1
<input type="button" value="Save"/> <input type="button" value="Clear"/>	

[← Return to Radius Servers list](#)

3. Edit the parameters you want to change and click **Save**.

## Monitoring with SNMP

You can configure your NSM3000 appliance for SNMP monitoring from a network operations server. The server can then issue periodic SNMP Get instructions to return the status of the NSM3000 appliance.

You configure SNMP on NSM appliances with access credentials for either SNMP v2c or SNMP v3. NSM3000 supports read-only access to the System Descriptor (sysDescr) and Host Resource MIB.

This section provides instructions for configuring NSM3000 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 NSM3000 appliance, select **System Administration > SNMP Monitoring**. The SNMP window appears. This window contains the tabs described in the following sections:

- SNMP Configuration on page 28
- SNMP System Information on page 29
- SNMP Trap Configuration on page 30

### SNMP Configuration

To configure SNMP:

1. Select **System Administration > SNMP Monitoring**.
2. Select the **SNMP Config** tab, which is shown in Figure 33 on page 29.

Figure 33: 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.

NSM3000 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 NSM 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 34 on page 29.

Figure 34: 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 35 on page 30.

Figure 35: Configuring SNMP Traps

Trigger	Value
<input checked="" type="checkbox"/> Disk space low	15 percent
<input checked="" type="checkbox"/> Memory low	20 percent
<input checked="" type="checkbox"/> CPU high	85 percent
<input checked="" type="checkbox"/> NSM start / stop	
<input checked="" type="checkbox"/> Admin Logon / Logoff	
<input checked="" type="checkbox"/> External IP Unreachable	

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

NSM3000 provides a simple mechanism for configuring syslog messaging between the 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, NSM3000 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 31
- Adding and Configuring Syslog Receivers on page 32
- Editing Syslog Receiver Configurations on page 34
- Deleting Syslog Receivers on page 34

### Viewing Syslog Receivers

To view the syslog receivers configured on your NSM3000 appliance, follow these steps:

1. Select **System Administration > Syslog Forwarding**. The Syslog Forwarding window appears. Figure 36 on page 33 shows an example.

### Syslog Forwarding

Select all. | Invert selection. | Add new Receiver

Receiver	Address	Type	System	Device Server	GUI Server	HA Server
<input type="checkbox"/> server1	1.2.3.4	UDP	maillog, updates	datacollector.log, ddhnspl.log, deviceDaemon.0, deviceservice.log, gproDDM.log	generateMPK.0, gproGDM.log, license.log, statusMonitor.0	highAvail.0
<input type="checkbox"/> sever2	1.2.3.5	UDP	messages			

Select all. | Invert selection. | Add new Receiver

Delete selected receivers

#### NSM Data Sources

GUI Server Log	Syslog facility
fingerprintMPK.0	user
generateMPK.0	user
gproGDM.log	user
guiDaemon.0	user
license.log	user
nbiservice.log	user
pro.mc.log	user
statusMonitor.0	user
webproxy.log	user
xdbservice.log	user

Device Server Log	Syslog facility
datacollector.log	user
ddhnspl.log	user

- View the configured syslog receivers in the table in the top portion of the window. Table 3 on page 32 describes the fields.

**Table 3: Viewing Syslog Receivers**

Field	Description
Receiver	A name provided by the network administrator to identify the syslog receiver
IP Address	The IP address of the syslog receiver
Type	The protocol used for forwarding messages: UDP, TCP, SSL
Data sources	The data sources configured for forwarding
System	The system logs configured to be sent to this receiver.
Device Server	The Device Server logs configured to be sent to this receiver.
GUI Server	The GUI Server logs configured to be sent to this receiver.
HA Server	The HA Server logs configured to be sent to this receiver.

### Adding and Configuring Syslog Receivers

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

- Select **System Administration > Syslog Forwarding**.
- 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.
- Click **Save**.
- Click **Add new Receiver**.

The syslog receiver configuration window appears as shown in Figure 36 on page 33.

Figure 36: Configuring a Syslog Receiver

**Syslog Receiver**

**Name:**

**IP:**

**Transport:**  UDP  TCP  SSL

---

**Data Sources**

**System Logs**

Console messages

Mail log

System updates

---

**NSM**

GUI Server Log	Syslog facility
<input type="checkbox"/> fingerprintMPK.D	user
<input checked="" type="checkbox"/> generateMPK.D	user
<input checked="" type="checkbox"/> gproGDM.log	user
<input type="checkbox"/> guiDaemon.D	user
<input checked="" type="checkbox"/> license.log	user
<input type="checkbox"/> nbiservice.log	user
<input type="checkbox"/> pro.mc.log	user
<input checked="" type="checkbox"/> statusMonitor.D	user
<input type="checkbox"/> webproxy.log	user
<input type="checkbox"/> xdbservice.log	user

Device Server Log	Syslog facility
<input checked="" type="checkbox"/> datacollector.log	user
<input checked="" type="checkbox"/> ddhosp.log	user
<input checked="" type="checkbox"/> deviceDaemon.D	user
<input checked="" type="checkbox"/> deviceservice.log	user
<input checked="" type="checkbox"/> gproDDM.log	user
<input type="checkbox"/> newLogWalker.D	user
<input type="checkbox"/> pro.dc.log	user
<input type="checkbox"/> profilerMgr.D	user
<input type="checkbox"/> statusMonitor.D	user

HA Server Log	Syslog facility
<input type="checkbox"/> backup.log	user
<input type="checkbox"/> ha.log	user
<input checked="" type="checkbox"/> highAvail.D	user

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 NSM 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**.

NSM3000 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 NSM3000 version.
- Add or modify proxy settings for the Yum server.

## Managing Users

The NSM3000 WebUI allows you to create multiple users with role-based access control to the WebUI. You can create a user in the WebUI and associate the user to a predefined user profile. You can also map a user created in the NSM3000 OS to a predefined user profile in the WebUI. However, this user profile is only applicable to the local OS user in the WebUI.



**NOTE:** You need System Administration permission to create users.

This topic contains the following sections:

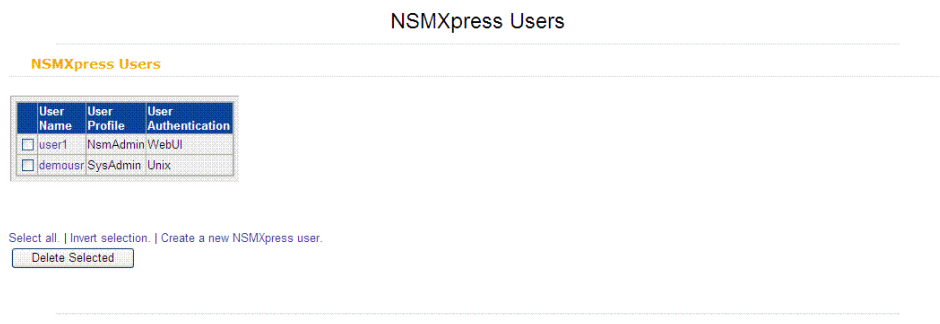
- Creating New NSM3000 Users on page 35
- Deleting a User on page 37
- Editing User Attributes on page 37
- Understanding User Profiles on page 37

### Creating New NSM3000 Users

To create a local OS user:

1. Select **System Administration > User Management**. The NSMExpress Users dialog box appears listing all NSM3000 users. See Figure 37 on page 35.

**Figure 37: NSMExpress Users Dialog Box**



2. Click **Create a new NSMExpress User**. The Create NSMExpress user dialog box appears. See Figure 38 on page 36.

Figure 38: Create NSMXpress User Dialog Box

Module Index Create NSMXpress User

---

**Create New User**

**Username**

**Password** Unix authentication

**Confirm Password**

**User Profile** NsmAdmin

[Return to user list](#)

3. Enter the user name in the **Username** text box.
4. Select **Unix authentication** from the **Password** drop-down list. The Password and Confirm Password text boxes will be disabled since the password will be fetched from the local OS.
5. From the **User Profile** drop-down list box, select the user profile you want to associate with the local user in the WebUI.
6. Click **Submit**. The NSMXpress Users dialog box appears with the new NSM appliance user listed.

To create a WebUI user:

1. Select **System Administration > User Management**. The NSMXpress Users dialog box appears listing all NSM appliance users. See Figure 39 on page 36.

Figure 39: NSMXpress Users Dialog Box

NSMXpress Users

---

NSMXpress Users

User Name	User Profile	User Authentication
<input type="checkbox"/> user1	NsmAdmin	WebUI
<input type="checkbox"/> demouser	SysAdmin	Unix

Select all | Invert selection | Create a new NSMXpress user.

2. Click **Create a new NSMXpress User**. The Create NSMXpress user dialog box appears.
3. Enter a user name in the **Username** text box.
4. Select **Set to** from the password drop-down list and enter the password you want to set in the password text box.
5. Reenter the password in the **Confirm Password** text box.

6. Select the user profile you want to associate with this user from the **User Profile** drop-down list box.
7. Click **Submit**. The NSMXpress Users dialog box appears with the new NSM appliance users listed.

### Deleting a User

To delete a user:

1. Select **System Administration > User Management**. The NSMXpress Users dialog box appears listing all NSM appliance users.
2. Select the check box next to the name of the user you want to delete and click **Delete Selected**. Click **Delete User** in the Delete Users confirmation dialog box that appears.



NOTE: You cannot delete admin users or change their user profiles.

### Editing User Attributes

To edit user attributes:

1. Select **System Administration > User Management**. The NSMXpress Users dialog box appears, with all NSM appliance users listed.
2. Click on the name of the user whose attributes you want to edit. The Edit NSMXpress Users dialog box appears.
3. Edit the parameters you want to change and click **Submit**. You can change the password and the user profile.

### Understanding User Profiles

NSM3000 provides four predefined user profiles that allow you to implement role-based access control over the NSM appliance WebUI. A user created via the WebUI or in the RADIUS server can be associated with any one of the following profiles:

- System Administrator—System Administrators are superusers with full access to all modules in the NSM3000 WebUI.
- NSM Administrator—NSM Administrators have access to NSM Administration, RADIUS Management, Maintenance and Troubleshooting modules.
- Network Operator—Network Operators have access to Network Utilities and Report Generation Modules.
- Guest User—Guest Users have read access to System Information and System Statistics modules.

When a user logs in, NSM3000 modules are displayed or hidden based on the user profile and the permissions associated with the profile. For more details about user profiles and permissions, see Table 4 on page 38.

Table 4: NSM3000 WebUI User Profiles and Permissions

NSM Appliance Modules	System Administrator	NSM Administrator	Network Operator	Guest User
<b>System Administration</b>				
Bootup and Shutdown	Yes	No	No	No
Change User Password	Yes	No	No	No
Network Configuration	Yes	No	No	No
Radius Management	Yes	Yes	No	No
SNMP Monitoring	Yes	No	No	No
Syslog Forwarding	Yes	No	No	No
System Time	Yes	No	No	No
System Update	Yes	No	No	No
User Management	Yes	No	No	No
WebUI Configuration	Yes	No	No	No
<b>NSM Administration</b>				
Change NSM Super User Password	Yes	Yes	No	No
Download NSM MIBs	Yes	Yes	No	No
Export Audit Logs	Yes	Yes	Yes	No
Export Device Logs	Yes	Yes	Yes	No
Generate Reports	Yes	Yes	Yes	No
NSM Configuration Files	Yes	Yes	No	No
NSM Database Backup	Yes	Yes	No	No
NSM Management IP	Yes	Yes	No	No
Schedule Security Updates	Yes	Yes	No	No
<b>Maintenance</b>				
System Statistics	Yes	Yes	Yes	Yes
<b>Troubleshooting</b>				
Action Audit Logs	Yes	Yes	No	No

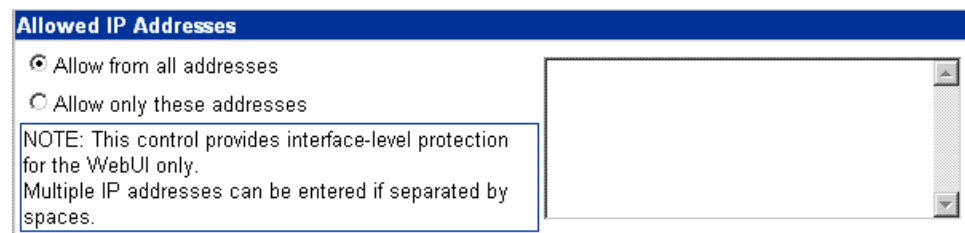
Table 4: NSM3000 WebUI User Profiles and Permissions (*continued*)

NSM Appliance Modules	System Administrator	NSM Administrator	Network Operator	Guest User
Error Logs	Yes	Yes	Yes	No
Network Utilities	Yes	Yes	Yes	No
Tech Support	Yes	Yes	Yes	No
System Information	Yes	Yes	Yes	Yes

## Configuring the Web Interface

To specify which NSM client computers can access NSM3000 through the Web interface, select **System Administration > WebUI Configuration**. The Allowed IP Addresses window appears as shown in Figure 40 on page 39.

Figure 40: Web Interface Access



## Maintaining NSM3000

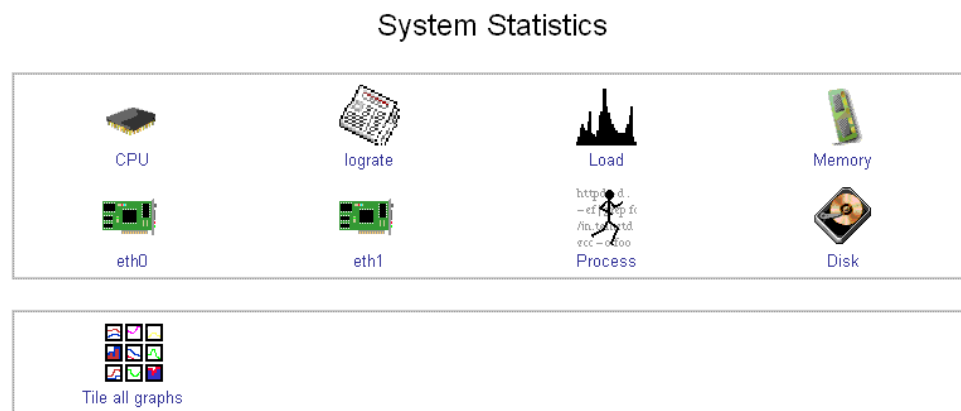
The Maintaining section of the NSM3000 navigation tree allows you to perform the tasks described in the following sections:

- Viewing System Statistics on page 39
- Upgrading the Recovery Partition on page 40

### Viewing System Statistics

To view system statistics, select **System Administration > Maintenance > System Statistics**. The system Statistics window appears as shown in Figure 41 on page 40.

Figure 41: 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.

## Upgrading the Recovery Partition

The recovery partition contains all files necessary to perform a clean installation of the NSM3000 OS and its applications with default settings. It provides a last-resort recovery

mechanism. When the NSM3000 appliance is shipped from the factory, the recovery partition files match the version of the NSM3000 OS with factory default settings.

Using the Recovery Upgrade option, you can make the current version of NSM3000 available for recovery, replacing the existing files in the recovery partition. The factory default recovery files are retained as an alternative recovery choice. Other versions are deleted.

Recovery upgrade uses two sets of packages to create a set of files from which you can perform a clean installation. One set makes up the NSM3000 OS, the other a set of upgrade script packages. Both sets are usually retained in the local file system. The NSM3000 OS set can also be downloaded from the Juniper Networks software repository.

NSM3000 splits the recovery upgrade process into a preparation phase and an upgrade phase. In the preparation phase, NSM3000 assembles a copy of the current version of the image files in a temporary workspace. In the upgrade phase, NSM3000 replaces the old recovery image files, and installs the current version of the image files from the temporary workspace into the recovery partition. By splitting the process into two phases, NSM3000 minimizes the period of vulnerability while the upgrade itself takes place.

To upgrade the recovery partition, follow these steps:

1. Select **System Administration > Maintenance > Update Recovery Partition**.

If the new recovery partition files have already been prepared, then the Upgrade screen appears. Proceed with the upgrade phase as described in step 5.

If the upgrade files have not yet been prepared, the Upgrade Preparation window appears. Proceed with the preparation phase in step 2.

2. Enter the location of the NSM3000 Regional server or Central Manager upgrade zip file, downloaded from the Juniper Customer Support Center when upgrading NSM, on the local file system.
3. If the NSM3000 Offline server upgrade file is available on the local file system, enter the location and name of the NSM3000 offline server upgrade file in the System upgrade source field. If the NSM3000 offline server upgrade file is not available on the local file system and the appliance has access to the Juniper Update site, select **Online**.

4. Click **Prepare System**.

The Preparation Progress screen shows the progress of the operation.

Errors are reported if the required files are unavailable, disk space is not sufficient, or the previous version files are invalid.

When preparation is completed, the Upgrade window appears.

5. In the Upgrade window, enter the admin Web UI password and then click **Start Update**.

The upgrade process usually takes less than one minute.



**CAUTION:** Do not interrupt the upgrade process. If you do, your NSM3000 appliance might not boot normally.

## Troubleshooting

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

- Auditing User Operations on page 42
- Error Logs on page 44
- Network Utilities on page 44
- Tech Support on page 47

### Auditing User Operations

You can audit all user operations performed in NSM3000. Users with System Administrator and NSM administrator permissions can view all Actions Logs in NSM3000.

To view Action Audit Logs:

1. Select **Troubleshooting > Action Audit Logs**. The NSMXpress Actions Log dialog box appears. See Figure 42 on page 42.

**Figure 42: NSMXpress Actions Dialog Box**

NSMXpress Actions Log

Search the NSMXpress log for actions ..

Search

Actions by NSMXpress users

- By any user
- By user
- By any user except

Actions by user profile

- By any profile
- By profile
- By any profile except

Actions by authentication mechanism

- By any authentication
- By authentication
- By any authentication except

Actions in module

- In any module
- In module

Actions on dates

- At any time
- For today only
- For yesterday only
- During the last week
- Between  and

2. Select the Action Audit Logs that you want to view:

- **Actions by NSMExpress Users:** Select the **By any user** check box to select actions by all users. Select the **By user** check box and choose a username from the drop-down list to specify actions by a particular user. Select **By any user except** and choose a username from the drop-down list to exclude actions by a specific user.
  - **Actions by User Profile:** Select the **By any profile** check box to select actions by all user profiles. Select the **By profile** check box and choose a profile from the drop-down list to specify actions by a specific user profile. Select **By any profile except** and choose a profile from the drop-down list to exclude actions by a user profile.
  - **Actions by authentication mechanism:** Select the **By any authentication** check box to select actions by all authentication mechanisms. Select the **By authentication** check box and choose an authentication mechanism from the drop-down list to specify actions by a specific authentication mechanism. Select **By any authentication except** and choose a profile from the drop-down list to exclude actions by an authentication mechanism.
  - **Actions in module:** Select the **In any module** check box to select actions in all modules. Select the **In module** check box and choose a module from the drop-down list to specify actions in a particular module.
  - **Actions on dates:** Select the **At any time** check box to select actions at any time. Select the **For today only** check box to select today's actions. Select the **For yesterday only** check box to select yesterday's actions. Select the **During the last week** check box to select last week's actions. Select the **Between** check box and enter the start date and end date in the drop-down list to view actions within the specified time period.
3. Click **Search**. The Search Results dialog box appears with the result of your query. See Figure 43 on page 43.

**Figure 43: Search Results Dialog Box**

Module Index		Search Results					
Logged actions on 14/Aug/2009 ...							
Action	Module	User	User profile	User Authentication	Client Address	Date	Time
Created NSMExpress user demouzz	User management	admin	SysAdmin	Unix	10.206.144.154	14/Aug/2009	04:11
Created NSMExpress user user1	User management	admin	SysAdmin	Unix	10.206.144.154	14/Aug/2009	04:11
Deleted Radius Server thirty-five	Radius Management	shaleen	SysAdmin	Radius	10.206.146.216	14/Aug/2009	00:53
Deleted 1 NSMExpress users	User management	shaleen	SysAdmin	Radius	10.206.146.216	14/Aug/2009	00:52
Added Radius Server thirty-five	Radius Management	admin	SysAdmin	Unix	10.206.146.216	14/Aug/2009	00:39
Created NSMExpress user sanjay	User management	admin	SysAdmin	Unix	10.206.146.216	14/Aug/2009	00:37

← Return to search form

## Error Logs

To review error logs, select **Troubleshooting > Error Logs**. Figure 44 on page 44 shows an example,

Figure 44: Review Error Logs

### System Logs

Log File	Description	
File /usr/netscreen/DevSvr/var/errorLog/deviceDaemon.0	Device Server Error Log	<a href="#">View..</a>
File /usr/netscreen/DevSvr/var/errorLog/pro.dc.log	Data Collector Error Log	<a href="#">View..</a>
File /usr/netscreen/DevSvr/var/errorLog/gproDDM.log	Device Directive Manager Error Log	<a href="#">View..</a>
File /usr/netscreen/DevSvr/var/errorLog/newLogWalker.0	Log Walker Error Log	<a href="#">View..</a>
File /usr/netscreen/DevSvr/var/errorLog/profilerMgr.0	Profiler Manager Error Log	<a href="#">View..</a>
File /usr/netscreen/DevSvr/var/errorLog/statusMonitor.0	Status Monitor	<a href="#">View..</a>
File /usr/netscreen/GuiSvr/var/errorLog/guiDaemon.0	Gui Server Error Log	<a href="#">View..</a>
File /usr/netscreen/GuiSvr/var/errorLog/pro.mc.log	Master Controller Error Log	<a href="#">View..</a>
File /usr/netscreen/GuiSvr/var/errorLog/gproGDM.log	Gui Directive Manager Error Log	<a href="#">View..</a>
File /usr/netscreen/GuiSvr/var/errorLog/statusMonitor.0	GuiSvr Status Monitor Error Log	<a href="#">View..</a>
File /usr/netscreen/HaSvr/var/errorLog/highAvail.0	High Avail Error Log	<a href="#">View..</a>

To view details of an individual error log, select the file you want to view and click **View**. Figure 45 on page 44 shows sample error log details.

Figure 45: Error Log Detail

[Module Index](#)

### View Logfile

`/usr/netscreen/DevSvr/var/errorLog/gproDDM.log`

Last  lines of Only show lines with text

```
cat: /usr/netscreen/DevSvr/var/errorLog/gproDDM.log: No such file or directory
```

Last  lines of Only show lines with text

## 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 46 on page 44.

Figure 46: Network Utilities Options



### Ping

Ping is a tool for checking network connectivity. NSM3000 prompts with questions so you can focus your search.

Figure 47 on page 45 shows an example.

Figure 47: Ping Utility

[Module Index](#)  
[Help..](#)

## Ping

Hostname   Verbosity Output?  Numeric Output only?  Bypass routing tables?

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 through 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

NSM3000 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 48 on page 46.

Figure 48: Traceroute Utility

[Module Index](#)  
[Help..](#)

## Traceroute

Hostname:

<input type="checkbox"/> Verbosity Output? <input type="checkbox"/> Numeric Output only? <input type="checkbox"/> Bypass routing tables? <input type="checkbox"/> Use ICMP instead of UDP? <input type="checkbox"/> Toggle Checksums? <input type="checkbox"/> Socket level debugging?	How many Hops? <input style="width: 50px;" type="text" value="30"/> Packet Length? <input style="width: 50px;" type="text" value="40"/> How many sec between sending each packet? <input style="width: 50px;" type="text" value="5"/> Initial time-to-live? <input style="width: 50px;" type="text" value="1"/> Interface: <input style="width: 50px;" type="text"/>
---	--



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 49 on page 46). The query type drop-down list contains several types of records found in the DNS database. Enter a name server or select the default. If you choose the default, nslookup uses the server on which NSM3000 is installed.

Figure 49: Lookup Utility

[Module Index](#)  
[Help..](#)

## Lookup

Hostname

Typ:

Nameserver:  Default

Timeout?

### 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 50 on page 47). When you calculate a netmask by the number of hosts, NSM3000 returns the smallest network available.

Figure 50: IP Subnet Calculator

**Calculate Netmask by Class and Bits**

Class:  Subnet Bits:

**Calculate Netmask by Number of Hosts**

Number of Hosts:

## 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**. NSM3000 creates a file you can download and send to Juniper Networks technical support. See Figure 51 on page 47.

Figure 51: Juniper Tech Support

**Tech Support**

**JTAC WEBSITE:** <https://support.juniper.net>

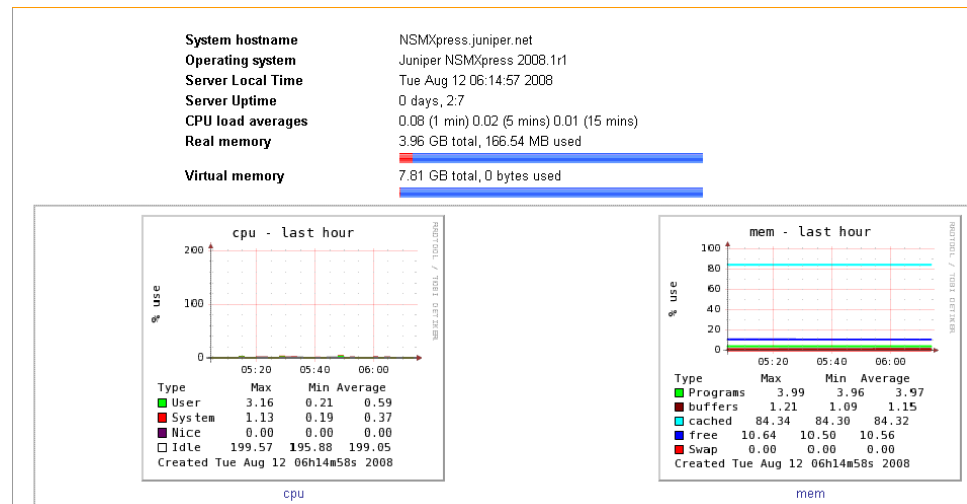
**JTAC PHONE NUMBER:** 1-888-314-JTAC

**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 52 on page 48.

Figure 52: System Information



## List of Technical Publications

Table 5 on page 48 describes the documentation for NSMxpress and NSM.

Table 5: Network and Security Manager Publications

Book	Description
<i>Network and Security Manager Installation Guide</i>	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.
<i>Network and Security Manager Administration Guide</i>	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 user interface (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.
<i>Network and Security Manager Configuring ScreenOS and IDP Devices Guide</i>	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.
<i>Network and Security Manager Online Help</i>	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.

Table 5: Network and Security Manager Publications (*continued*)

Book	Description
<i>Network and Security Manager API Guide</i>	Provides complete syntax and a description of the Simple Object Access Protocol (SOAP) messaging interface to NSM.
<i>Network and Security Manager Release Notes</i>	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.
<i>NSMExpress and NSM3000 User Guide</i>	Describes how to set up and manage NSM appliances 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/us/en/local/pdf/resource-guides/7100059-en.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: <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

---

October 27, 2009—Revision 1.

November 18, 2009—Revision 2.

Copyright © 2010, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks 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.