



Juniper Networks
NSMXpress

User Guide

Release 2007.3

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Part Number: 530-020830-01

Copyright Notice

Copyright © 2007 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Contents

	About This Guide	iii
	Audience	iv
	Conventions	iv
	Documentation	iv
	Related Documentation	iv
	Web Access	v
	Comments About the Documentation	v
	Contacting Customer Support	vi
Chapter 1	Getting Started	1
	About NSMXpress	2
	Installation and Configuration Workflow	2
	Hardware Installation	2
	Installing the Hardware	3
	LED Behavior	5
	Software Configuration	5
	NSMXpress Users	5
	Initial Setup Configuration	6
	Boot NSMXpress	6
	Set Up Your Appliance	7
	CLI Configuration	7
	Web Interface Configuration	8
Chapter 2	Installing NSM from the CLI	9
	Navigating the Main Menu	10
	General Options	10
	Using nsm_setup	11
	Configure the NSM Software	11
	Regional Server Configuration	12
	Typical Settings	12
	Remote Replication of Database	13
	Custom Settings	14
	High Availability	14
	Statistical Report Server Enabled	16
	Central Manager Configuration	17
	Remote Replication of Database	17
	High Availability	18
	Standard Configuration Options	20
	Change Password	20
	Set Interface Options	20
	Set Routing Options	21
	Change the NSMXpress Hostname	22
	Set DNS Servers	22

Change Time Options 22
 Forward Local Status E-mails 23
 System Security Update 23
 Saving Setup Options 23
 NSMXpress Default Restoration 24

Chapter 3 Configuring NSM from the Web Interface 27

Configuring the NSM Software 28
 Basic Settings 28
 Advanced Options 30
 Remote Replication of Database 30
 High Availability 31
 SRS Enabled Options 34
 Install NSM Software 35
 Managing NSM Administration 35
 Change the Superuser Password 36
 Download NSM MIBS 36
 Export Audit Logs 36
 Export Device Logs 37
 Generate Reports 37
 Modify NSM Configuration Files 38
 NSM Database Backup 38
 Change the NSM Management IP 39
 Schedule Security Updates 39
 Managing System Administration 40
 Reboot and Shut Down 40
 Change the User Password 40
 Configure the Network 40
 Network interfaces 41
 System Time 43
 System Updates 43
 Configure the Web Interface 43
 Maintenance 43
 System Statistics 43
 CPU 44
 Log Rate 44
 CPU Load 44
 Memory Data 44
 Network Data 44
 Process Count 44
 Disk Data 45
 Tile All Graphs 45
 Troubleshooting 45
 Error Logs 45
 Network Utilities 45
 Ping 46
 Traceroute 47
 Lookup 47
 IP Subnet Calculator 48
 Tech Support 48

About This Guide

Juniper Networks NSM*Xpress* is an appliance version of Netscreen-Security Manager (NSM), a software application that centralizes control and management of your Juniper Networks security devices. With NetScreen-Security Manager, Juniper Networks delivers integrated, policy-based security and network management for all security devices. NSM*Xpress* runs NSM 2007.3.

NSM*Xpress* simplifies the complexity of security device administration by providing a single, integrated management interface that controls every device parameter. Each appliance is preconfigured as either a regional server or central manager.

This guide describes how you can install NSM onto an appliance. In addition, this guide describes how to manage the appliance using the NSM*Xpress* command-line interface (CLI) or the Web interface.

This preface contains the following sections:

- Audience on page iv
- Conventions on page iv
- Documentation on page iv
- Contacting Customer Support on page vi

Audience

This guide is intended for system administrators responsible for the security infrastructure of their organization. Specifically, this book discusses concepts of interest to firewall and VPN administrators; network or security operations center administrators; and system administrators responsible for user permissions on the network.

Conventions

The sample screens used throughout this guide are representations of the screens that appear when you install and configure the NSM and NSMXpress. The actual screens may differ.

Table 1 shows the text conventions used in this guide.

Table 1: Text Conventions

Convention	Description	Examples
Bold typeface	Represents commands and key strokes in text.	<ul style="list-style-type: none"> ■ Click Submit. ■ Enter sudo su - nsm.
<i>Italics</i>	<ul style="list-style-type: none"> ■ Identify book names ■ Used in a product name 	<ul style="list-style-type: none"> ■ NetScreen-Security Manager 2007.3 Administrator's Guide ■ NSMXpress

Documentation

This guide contains the following chapters:

- Chapter 1, “Getting Started”—This chapter shows how to install the hardware and set up the appliance for installing NSM software.
- Chapter 2, “Installing NSM from the CLI”—This chapter shows how to install NSM software on the appliance using the command-line interface (CLI).
- Chapter 3, “Configuring NSM from the Web Interface”—This chapter shows how to install NSM software on the appliance and how to manage NSM using the Web interface.

Related Documentation

The NetScreen-Security Manager documentation includes the following guides:

- *NetScreen-Security Manager 2007.3 Administrator's Guide*—This guide describes how to use and configure key management features in the NetScreen-Security Manager. It provides conceptual information, suggested workflows, and examples where applicable. This guide is best used in conjunction with the NetScreen-Security Manager Online Help, which provides step-by-step instructions for performing management tasks in the NetScreen-Security Manager user interface.

- *NetScreen-Security Manager Installer Guide*—This guide details the steps to install the NetScreen-Security Manager management system on a single server or on separate servers. It also includes information on how to install and run the NetScreen-Security Manager user interface. This guide is intended for IT administrators responsible for the installation and/or upgrade to NetScreen-Security Manager.
- *NetScreen-Security Manager: Configuring Firewall/VPN Devices*—This guide details how to create a device configuration, including zones, interfaces, and routes. It also details how to create VPN components such as protected resources and IKE proposals, and guides you through building VPNs at the system level and at the device level.
- NetScreen-Security Manager Online Help—The online Help provides task-oriented procedures that describe how to perform basic tasks in the NetScreen-Security Manager user interface. It also includes a brief overview of the NetScreen-Security Manager system and a description of the GUI elements.

The online Help is best used in conjunction with the *NetScreen-Security Manager 2007.3 Administrator's Guide*, which provides conceptual information, suggested workflows, and examples for management tasks where applicable.

The online Help is intended for network and security administrators who are using the user interface to configure and manage devices.

- NetScreen-Security Manager Release Notes—The release notes provide 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 Web.

Web Access

To obtain technical documentation for any Juniper Networks security product, visit www.juniper.net/techpubs/.

Comments About the Documentation

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation to better meet your needs. E-mail your comments to:

- techpubs-comments@juniper.net

Along with your comments, be sure to indicate:

- Document name
- Document part number
- Page number
- Software release version

Contacting Customer Support

For technical support, contact Juniper Networks at support@juniper.net, or at 1-888-314-JTAC (within the United States) or 408-745-9500 (from outside the United States).

Chapter 1

Getting Started

Thank you for choosing NSMXpress as your Juniper Networks NetScreen-Security Manager (NSM) appliance. This version of NSMXpress comes pre-installed as a regional server or central manager.

This chapter contains the following sections:

- About NSMXpress on page 2
- Hardware Installation on page 2
- Software Configuration on page 5
- Initial Setup Configuration on page 6

About NSMXpress

NSMXpress is an appliance version of NetScreen-Security Manager (NSM) and runs NSM 2007.3. NSMXpress simplifies the complexity of security device administration by providing a single, integrated management interface that controls every device parameter.

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 security management solution.

NSMXpress makes it easy for administrators to control all aspects of Juniper's firewall/VPN and intrusion detection and prevention (IDP) devices, including device configuration, network settings, and security policy.

Installation and Configuration Workflow

This guide documents the following workflow 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 either the CLI or the Web interface.
4. Configure NSM software, which was pre-installed onto the NSMXpress appliance, with site-specific parameters.

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.

Table 2 provides required port information on the NSMXpress.

Table 2: Required Ports on NSMXpress

Direction	Port	Description	LAN	Internet	Depends on Configuration
In	22	SSH command-line management	Yes	No	No
	443	Web interface	Yes	No	No
	7800	Connections from managed devices to NSMXpress	Yes	Yes	No
	7801	Connections from the NSM GUI Client to NSMXpress	Yes	No	No
	7802	Heartbeat between peers in an HA cluster	Yes	No	Yes
	7803	Connections from managed IDP devices to NSMXpress.	Yes	Yes	Yes
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	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
	7802	Heartbeat between peers in an HA Cluster	Yes	No	Yes

Sites with devices running ScreenOS 4.0 may require additional ports. For more information, refer to the *NetScreen-Security Manager Administrator's Guide*.

Installing the Hardware

Place the shipping container on a flat surface and remove the hardware components with care. Remove the NSMXpress device from the shipping container and place it on a flat surface.

To install NSMXpress:

1. Mount NSMXpress in your server rack using the attached mounting brackets.
2. Plug the power cord into the AC receptacle on the rear panel. See Figure 1.

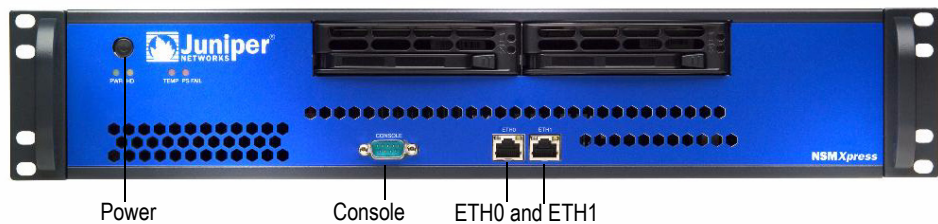
If your NSMXpress contains two power supplies, plug a power cord into each of the AC receptacles.

Figure 1: Rear Panel of NSMXpress

3. 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 in the event that one of the power circuits fails.

4. Plug the Ethernet cable into the port marked ETH0 (for internal) on the front panel. See Figure 2.

Figure 2: Front Panel of NSMXpress

Once you apply power to the NSMXpress, the internal port uses two LEDs to indicate the LAN connection status, which is described in Table 3, "Ethernet Port LEDs," on page 5.

5. Plug the null modem serial cable into the console port. See Figure 3.

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

Figure 3: Console Port on Front Panel

6. 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.

Hardware installation is now complete. The next step is to perform an initial setup as described in "Software Configuration," on page 5.

LED Behavior

Table 3 provides LED information on the ETH0 and ETH1 ports.

Table 3: Ethernet Port LEDs

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

Software Configuration

NSMXpress runs NetScreen-Security Manager 2007.3. After logging in as “admin”, an initial setup script walks you through the configuration, which requires the following information:

- A new password
- The IP address
- The default route

The setup menu then allows you to configure additional system settings before finalizing the installation process.

NSMXpress Users

NSMXpress has three user levels. All users log in as the “admin” user. To use the command line to administer NSM, change to the “nsm” user. For advanced administration, change to the “root” user.

The following users are available to manage NSMXpress.

- **“admin” user**—Logs into the NSMXpress setup program and changes to “nsm” user or “root” user from the command line.
- **“nsm” user**—Administers NSM services. To change to the “nsm” user from the “admin” user, go to the \$ prompt, enter **sudo su - nsm** for the \$ nsm prompt, then enter the “admin” password you set when logging into the NSMXpress appliance. To return to the “admin” user, enter **exit** from the \$ prompt.
- **“root” user**—Administers advanced system settings. To change to “root” user from the “admin” user, go to the \$ prompt, enter **sudo su - root** for the # root prompt, then enter the “admin” password you set when logging into the NSMXpress appliance. To return to the “admin” user, enter **exit** from the # prompt.

Initial Setup Configuration

When you first power up 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 NSMXpress for the first time. The workflow is as follows:

- Boot NSMXpress on page 6
- Set Up Your Appliance on page 7

Boot NSMXpress

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

When NSMXpress 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. See Figure 4.

Figure 4: Initial Login Screen for NSMXpress

```

Juniper NSMXpress release NSM 2007.3
Kernel 2.6.9-42.0.3.ELsmp on an i686

NSMXpress.juniper.net login:
```

NOTE: Allow the setup script to fully run before proceeding to the next step.

4. Enter **admin** as your default login name and press Enter.
5. Enter **abc123** as your default password and press Enter.
6. Change your default password when prompted.

7. 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.

NSMXpress comes preconfigured either as a regional server or a central manager. Figure 5 shows the appliance as a regional server.

Figure 5: An NSMXpress Regional Server

```
--- NSM operational mode ---
Your NSMXpress appliance is a Regional Server.

Please enter new IP address for interface eth0
█
```

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 gateway address for interface eth0 and press Enter.

NSMXpress allows you to configure your appliance using the CLI or the Web interface. Figure 6 shows the options available to you once you complete setting up the appliance.

Figure 6: NSMXpress After Completing Initial Setup

```
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://172.24.68.111/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.

[admin@NSMXpress ~]#
```

You have completed setting up your NSMXpress appliance. To complete the setup process using the CLI, go to “CLI Configuration,” on page 7. To complete the setup process using the Web interface, go to “Web Interface Configuration,” on page 8.

CLI Configuration

To configure NSM on your system from the CLI use the following steps. If you are logged in, enter **nsm_setup** at the command prompt.

1. Enter your admin user name and then press Enter. See Figure 7.

Figure 7: NSMXpress Login

```

Juniper NSMXpress OS build 2.105498
NSM 2007.3r1
Kernel 2.6.9-55.0.2.ELsmp on an i686

NSMXpress.juniper.net login: admin
Password:
Last login: Mon Nov 26 17:20:25 on ttyS0
Run NSMXpress system setup? [y/N]

```

2. Enter your password and then press Enter.
3. Enter **y** to run the system setup program from the CLI.

NOTE: These values are not case-sensitive, however, the uppercase N indicates it is the default value. Any keystroke including Enter (but not y or Y), accepts the default value.

4. Go to Chapter 2, “Installing NSM from the CLI,” for details on how to install and configure NSM on your NSMXpress appliance from the CLI.

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. See Figure 8.

Figure 8: Web Interface Login URL

```

Your NSMXpress appliance is on the network.
To configure your system via a web browser, connect to:
https://172.24.68.111/admin
To configure your system via command line, type:
nsm_setup

```

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. Go to Chapter 3, “Configuring NSM from the Web Interface,” for details on how to install and configure NSM on your NSMXpress appliance from the Web interface.

Chapter 2

Installing NSM from the CLI

This chapter describes how to install and configure NSM on your NSMXpress appliance from command-line interface (CLI). It contains the following sections:

- Navigating the Main Menu on page 10
- Configure the NSM Software on page 11
- Regional Server Configuration on page 12
- Central Manager Configuration on page 17
- Standard Configuration Options on page 20
- NSMXpress Default Restoration on page 24

Navigating the Main Menu

As you configure your NSMXpress, the following standard navigational menu options are available to you. This section provides information on general options you can use during setup and configuration. These include:

- General Options on page 10
- Using nsm_setup on page 11

General Options

Figure 9 shows a main menu with general options available.

Figure 9: NSM Configuration Main Menu Options

```
NSM Configuration Main Menu
1> Management IP [10.10.10.10]
   The IP address on this server that will be
   used for management
2> NSM "super" password []
   Password for "super" user
3> Menu: Remote Replication of Database [Off]
4> Menu: High Availability [Off]
5> Menu: SRS [Off]

A> Apply settings
C> Cancel all changes and quit
R> Redraw menu

Choice [1-5,A,C,R]:
```

To select an option, enter the number at the prompt and then press Enter. The following options are available on most menus:

- **Numbered Options**—Enter setting options by number (**1**, **2**, and so on) to access individual parameters or open menus.
- **Apply settings**—Enter **A** to apply and save any modifications you have made and takes you out of the setup program.
- **Cancel all changes and quit**—Enter **C** to take you out of the setup program without saving any changes you made since you last saved.
- **Redraw menu**—Enter **R** to redraw the screen text.
- **Main Menu/Return to Main Menu**—Enter **M** to return to the main menu. Most menus will have this option as the last options on the numbered list of options.
- **Quit**—Enter **Q** to take you out of the setup program, after which you will be prompted to save or cancel any changes you made since you last saved. See Figure 10.

Figure 10: Quitting the Setup Program

```
Q> Quit
R> Redraw menu
Choice [1-9,Q,R]: Q
```

Using `nsm_setup`

After initial setup, you can cancel out of the NSMXpress setup program and later return to it. The steps in the following procedure assume NSMXpress is connected to the computer running a terminal emulation program. If not, see “Initial Setup Configuration,” on page 6 for details.

NOTE: Run `nsm_setup` with your “admin” user login only. Do not run `nsm_setup` as an “nsm” user.

To return to the setup program after the initial setup:

1. Turn on NSMXpress and wait for the login prompt. See Figure 11.

Figure 11: Initial Login Screen for NSMXpress

```
Juniper NSMXPress NSM 2007.3r1
Kernel 2.6.9-42.0.8.ELsmp on an i686

NSMXpress.juniper.net login: admin
Password:
Last login: Fri Jul 13 09:43:50 on ttyS0
Run NSMXPress system setup? [y/N] N

To start system setup manually, type:
nsm_setup

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

[admin@NSMXpress ~]$
```

2. Log in using your “admin” user name and password.
3. Enter `nsm_setup` at the prompt.
4. Enter your password and press Enter to return to the main menu.

Configure 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 section describes that setup process.

The steps in this procedure assume you:

- Have completed all appropriate steps in Chapter 1, “Getting Started.”
- Have a console terminal or terminal emulation utility running.

- See the command output as it appears in Figure 12, in the emulation utility window.

Figure 12: NSMXpress Startup Screen

```
Your NSMXpress is now active on the network.
To configure your system via a web browser, connect to:
  https://172.24.68.111/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.

[admin@NSMXpress ~]#
```

Your NSMXpress appliance comes preconfigured as a regional server or a central manager.

- Regional Server Configuration on page 12
- Central Manager Configuration on page 17

For more information on how to use NSMXpress and configuration options, to the following sections:

- Navigating the Main Menu on page 10
- Standard Configuration Options on page 20
- NSMXpress Default Restoration on page 24

Regional Server Configuration

If you want to configure the central manager go to “Central Manager Configuration,” on page 17. For details on using the general setup menu items to “Navigating the Main Menu,” on page 10.

After NSMXpress saves and applies your new system changes, you can configure the regional server. You can select one of the following options by number:

- **Typical Settings**—Enter **1** to select typical settings. This option provides a simplified menu to install regional server. When using these options neither HA nor statistical report server (SRS) can be in use.
- **Custom Settings**—Enter **2** to select custom settings. This option provides full access to all configuration options including HA and SRS for regional server.

Typical Settings

This section describes the options that are available for a typical installation for the regional server. See Figure 13.

Figure 13: Typical Settings for Regional Server

```
1> Management IP [10.150.43.204]
The IP address on this server that will be
used for management

2> NSM 'super' password [*****]
Password for 'super' user

3> NSM License type [Base_Install]
Specify a license file, or select "Base Install"
to use the built-in limited device license.

4> Menu: Remote Replication of Database [Off]
```

You have the following options:

- **Management IP**—Enter **1** to select interface eth0 or eth1 as the primary IP address for your management server. Once configured, the setup program displays the IP address for the interface you selected.
- **NSM 'super' password**—Enter **2** to specify an NSM 'super' password. This password must be at least eight characters long. There are no other requirements. However, this password is case sensitive. This password is used by the NSM 'super' user (also referred to as the NSM administrator). This user has the highest level of privileges in NSM.
- **NSM License type [Base Install]**—Enter **3** to the license option. Enter **Base Install** to use the built-in limited device license for as many as 25 devices. This option is the default. Otherwise, enter the files name of the license file you purchased from Juniper that permits you to manage more than 25 devices.
- **Menu: Remote Replication of Database**—Enter **4** to open a menu that allows you to mirror 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. See Figure 14.

Figure 14: Remote Replication of Database Menu

```
1> Remote Replication of Database [n]
If 'y', local backups will be sent to a remote backup machine

2> Hour of day to Replicate Database [02]
Hour to start a backup

3> Remote Backup IP []
IP address of a remote backup machine

4> Remote Replication Timeout (seconds) [1800]
Rsync Command Backup Timeout (seconds)
(Default is 1800 seconds)
```

Remote Replication of Database

The screen always shows the current status of the remote backup database. If there is no status, the option has not yet been configured.

- **Remote Replication of Database**—Enter **1** to turn remote replication on or off. Enter **y** to turn it on and enter **N** to turn it off.

- **Hour of day to Replicate Database**—Enter **2** to start the backup at the specified time. The valid range is 00-23.
- **Remote Backup IP**—Enter **3** to specify the IP address of the remote backup machine. Backup information is copied to the /var/netscreen/dbbackup directory on the remote server. The 'nsm' user must exist on both machines and you must establish an SSH trust relationship. See the *NetScreen-Security Manager Installer Guide* for details.
- **Remote Replication Timeout**—Enter **4** to time out the remote backup. The valid range is 1-65535 seconds.

Custom Settings

This section describes the custom options that are available for a regional server configuration. The custom options include the typical options described in the previous section as well as the two options shown in Figure 15.

Figure 15: Custom Settings for Regional Server

```
4> Menu: High Availability [Off]
5> Menu: SRS [Off]
```

You have the following options:

- **High Availability**—Enter **5** to open a menu to configure HA.
- **Statistical Report Server Enabled**—Enter **6** to open a menu to configure statistical report server (SRS).

NOTE: Juniper SRS is a complementary product to NSM and must be installed on a separate server.

High Availability

The following options are available to configure high availability (HA) on the regional server.

- **High Availability**—Enter **1** to turn HA on or off.
- **Primary Status**—Enter **2** to specify NSMExpress as either the primary or secondary server. If you select y, it is the primary server. If you select n, it is the secondary server.
- **HA Remote IP**—Enter **3** to specify the IP address for the HA peer in the HA cluster.
- **HA Link Failure Detection IP**—Enter **4** to specify the IP address of a machine outside of the HA cluster that you can ping to verify connection status.
- **HA Inter-server password**—Enter **5** to specify the heartbeat password used between the primary and secondary servers.

- **Menu: Shared Disk**—Enter **6** to open a menu to help you configure a shared disk (see Figure 16). NSMXpress supports shared disk with NFS only. Because of the data-intensive nature of NSM, we recommend gigabit speed links (1000 Mbps) for shared disk usage. For more information on options available to you for custom settings, refer to the *Netscreen-Security Manager Installer Guide*.

Figure 16: Shared Disk Menu

```

1> Shared Disk: Gui Server [n]
If 'y', data directory for GUI Server is a shared disk partition

2> Shared Disk: Device Server [n]
If 'y', data directory for Device Server is a shared disk partition

3> Shared Disk Source (NFS) []
Source of shared disk, e.g. /dev/sdc1 or server:/share

4> Shared Disk NFS Mount Options [rw]
Options when mounting shared disk e.g. rw, intr, tcp, soft, timeo=2

5> Return to High Availability menu

```

- **Menu: HA Links**—Enter **7** to open a menu to help you configure the second HA link in the HA cluster (see Figure 17). Use the items 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 “Set Interface Options,” on page 20 for more information). Setting a redundant link is optional. For more information on options available to you for custom settings, refer to the *Netscreen-Security Manager Installer Guide*.

Figure 17: HA Links Menu

```

1> HA Link count [2]
Number of heartbeat links between the Primary and Secondary
Servers.

2> HA Link 2 Local IP []
IP address for this machine's secondary heartbeat link

3> HA Link 2 Remote IP []
IP address for the peer's secondary heartbeat link

4> HA Remote Replication IP []
IP address used for remote HA replications

5> Return to High Availability menu

```

- **Menu: HA Advanced Settings**—Enter **8** to open a menu to configure HA advanced settings (see Figure 18). For more information on options available to you for custom settings, refer to the *Netscreen-Security Manager Installer Guide*.

Figure 18: HA Advanced Main Menu

```

1> HA Heartbeat Frequency [15]
Time interval in seconds between heartbeat messages (Default is 15
seconds)

2> HA Heartbeat Failure Threshold [4]
Number of missing heartbeat messages before automatic switchover
occurs (Default is 4 missing messages)

3> HA Data Replication Timeout [1800]
Rsync Command Replication Timeout (Default is 1800 seconds)

4> Return to High Availability menu

```

Statistical Report Server Enabled

The following options are available to configure statistical report server (SRS). See Figure 19.

NOTE: Juniper SRS is a complementary product to NSM and must be installed on a separate server.

Figure 19: SRS Menu

```

1> SRS [n]
Statistical Report Server will be used with this GUI Server

2> SRS DB IP []
Database server IP address

3> SRS DB Type [pgsql]
Database type

4> SRS Database Name [netscreen]
Database name

5> SRS DB Owner Name [netscreen]
Database user name

6> SRS DB Owner Password []
Database password

```

You have the following options:

- **SRS**—Enter **1** to turn the statistical report server on or off. Enter **y** to turn it on and enter **N** to turn it off. If you turn it on, the SRS will be used with the GUI Server.
- **SRS DB IP**—Enter **2** to specify the IP address for the server on which you have installed the SRS database server.
- **SRS DB Type**—Enter **3** to specify the database type. The options are `pgsql` (default), `oracle`, and `mssql`.
- **SRS Database Name**—Enter **4** to specify the name of the SRS database on the SRS server. The default value for this option is `netscreen`.
- **SRS DB Owner Name**—Enter **5** to specify the name of the SRS database owner. The default value for this option is `netscreen`.

- **SRS DB Owner Password**—Enter **6** to specify the owner password for the SRS database. There is a minimum of eight characters required. The password is case sensitive.

NOTE: Click **Submit** to save the options and return to the NSM Configuration Main Menu.

Central Manager Configuration

If you want to configure a regional server go to “Regional Server Configuration,” on page 12. For details on using the general setup menu items to “Navigating the Main Menu,” on page 10.

This section describes the options that are available for a central manager configuration. Figure 20 shows the central manager main menu options.

Figure 20: Central Manager Main Menu

```
1> Management IP [10.10.10.10]
   The IP address on this server that will be
   used for management

2> NSM "super" password []
   Password for "super" user

3> Menu: Remote Replication of Database [Off]

4> Menu: High Availability [Off]
```

You have the following options:

- **Management IP**—Enter **1** to select interface eth0 or eth1 as the primary IP address for your management server. Once configured, the setup program displays the IP address for the interface you selected.
- **NSM ‘super’ password**—Enter **2** to specify an NSM ‘super’ password. This password must be at least eight characters long. There are no other requirements. However, this password is case sensitive. This password is used by the NSM ‘super’ user (also referred to as the NSM administrator). This user has the highest level of privileges in NSM.
- **Menu: Remote Replication of Database**—Enter **3** to open a menu to configure remote replication of your database. See Figure 21.
- **Menu: High Availability**—Enter **4** to open a menu to configure HA.

Remote Replication of Database

This following options allows you to mirror 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. See Figure 21.

The screen always shows the current status of the remote backup database. If there is no status, the option has not yet been configured.

Figure 21: Remote Replication of Database Menu

```

1> Remote Replication of Database [n]
If 'y', local backups will be sent to a remote backup machine

2> Hour of day to Replicate Database [02]
Hour to start a backup

3> Remote Backup IP []
IP address of a remote backup machine

4> Remote Replication Timeout (seconds) [1800]
Rsync Command Backup Timeout (seconds)
(Default is 1800 seconds)

```

- **Remote Replication of Database**—Enter **1** to turn remote replication on or off. Enter **y** to turn it on and enter **N** to turn it off.
- **Hour of day to Replicate Database**—Enter **2** to start the backup at the specified time. The valid range is 00-23.
- **Remote Backup IP**—Enter **3** to specify the IP address of the remote backup machine. Backup information is copied to the /var/netscreen/dbbackup directory on the remote server. The 'nsm' user must exist on both machines and you must establish an SSH trust relationship. See the *NetScreen-Security Manager Installer Guide* for details.
- **Remote Replication Timeout**—Enter **4** to time out the remote backup. The valid range is 1-65535 seconds.

High Availability

The following options are available to configure high availability (HA).

- **High Availability**—Enter **1** to turn HA on or off.
- **Primary Status**—Enter **2** to set NSMXpress as either the primary or secondary server. If you select **y** for this option, it is the primary server. If you select **n**, it is the secondary server.
- **HA Remote IP**—Enter **3** to set the IP address for the HA peer in the HA cluster.
- **HA Link Failure Detection IP**—Enter **4** to set the IP address of a machine outside of the HA cluster that you can ping to verify connection status.
- **HA Inter-server password**—Enter **5** to set the heartbeat password used between the primary and secondary servers.
- **Menu: Shared Disk**—Enter **6** to open the Shared Disk menu.

The options in this menu (see Figure 22) help you configure shared disk. NSMXpress supports shared disk via NFS only. Due to the data-intensive nature of NSM, gigabit speed links (1000 Mbps) are highly recommended for Shared Disk usage. For more information on options available to you for custom settings, refer to the *Netscreen-Security Manager Installation Guide*.

Figure 22: Shared Disk Menu

```
1> Shared Disk: Gui Server [n]
If 'y', data directory for GUI Server is a shared disk partition

2> Shared Disk: Device Server [n]
If 'y', data directory for Device Server is a shared disk partition

3> Shared Disk Source (NFS) []
Source of shared disk, e.g. /dev/sdc1 or server:/share

4> Shared Disk NFS Mount Options [rw]
Options when mounting shared disk e.g. rw, intr, tcp, soft, timeo=2

5> Return to High Availability menu
```

- **Menu: HA Links**—Enter 7 to open the HA Links menu.

The options in this menu (see Figure 23) help you configure the second HA link in 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. Setting a redundant link is optional. For more information on options available to you for custom settings, refer to the *Netscreen-Security Manager Installation Guide*.

Figure 23: HA Links Menu

```
1> HA Link count [2]
Number of heartbeat links between the Primary and Secondary
Servers.

2> HA Link 2 Local IP []
IP address for this machine's secondary heartbeat link

3> HA Link 2 Remote IP []
IP address for the peer's secondary heartbeat link

4> HA Remote Replication IP []
IP address used for remote HA replications

5> Return to High Availability menu
```

- **Menu: HA Advanced Settings**—Enter 8 to open the HA advanced Settings menu (see Figure 24). For more information on how to set up HA advanced settings, refer to the *Netscreen-Security Manager Installation Guide*.

Figure 24: HA Advanced Settings Menu

```
1> HA Heartbeat Frequency [15]
Time interval in seconds between heartbeat messages (Default is 15
seconds)

2> HA Heartbeat Failure Threshold [4]
Number of missing heartbeat messages before automatic switchover
occurs (Default is 4 missing messages)

3> HA Data Replication Timeout [1800]
Rsync Command Replication Timeout (Default is 1800 seconds)

4> Return to High Availability menu
```

Standard Configuration Options

After the initial setup, continue with a typical configuration options that includes the following tasks:

- Change Password on page 20
- Set Interface Options on page 20
- Set Routing Options on page 21
- Change the NSMExpress Hostname on page 22
- Set DNS Servers on page 22
- Change Time Options on page 22
- Forward Local Status E-mails on page 23
- System Security Update on page 23
- Saving Setup Options on page 23

Follow the setup prompts on the main menu to set or modify these options. Your configuration options (with the exception of any password changes) will not take effect until you apply the changes.

Change Password

To change your password:

1. Enter **1** at the prompt.
2. Select **y** when prompted to change the password for an “admin” user.
3. Enter the new password and press Enter.
4. Retype the new password and press Enter.

Your password is changed and the setup program returns you to the main menu.

Set Interface Options

NSMExpress has two ports labeled ETH0 and ETH1. During initial setup, you set up the eth0 interface options. Use this menu to set interface options for eth1 or modify either interface.

NOTE: If you are going to use a second link, you need to configure an IP address for eth1 before configuring this setting.

To set or modify interface options:

1. Enter **2** at the prompt.

The menu shows the existing status of each interface.

2. Set or modify options for one of the interfaces by selecting one of the following options:
 - **1** to modify eth0.
 - **2** to set or modify eth1 .
3. Make the following selection for interface options by selecting one of the following options:
 - **1** to change the IP address and return to the main menu.
 - **2** to go to the next step.
4. Make the following selection for physical parameters (such as interface speed) by selecting one of the following options:
 - **1** to set the autonegotiate option and return to the main menu.
 - **2** to set the physical parameters manually and go to the next step.
5. Select the interface speed by selecting one of the following options:
 - **1** for 10 Mbps and go to the next step.
 - **2** for 100 Mbps and go to the next step.
 - **3** for 1000 Mbps and go to the next step.
6. Select **1** for full duplex or **2** for half duplex, then return to the main menu.

Set Routing Options

To set or modify routing options:

1. Select **3** from the main menu.
2. Select one of the following options:

- **1** to change default gateway options (optional).

Follow the prompts to change the IP address of the default gateway and return to the main menu.

- **2** to change the static routing options (optional).

Follow the prompts to add the new static route and return to the main menu.

Change the NSMXpress Hostname

To change the hostname:

1. Select **4** from the main menu.
2. Select **y** at the verification prompt, to continue.

If you do not want to change the hostname, enter **N** to return to the main menu.

3. Enter the new hostname and press Enter to return to the main menu.

Set DNS Servers

You can add up to three DNS servers. Enter each one using dotted decimal notation. Each addition returns you to the main menu. If you want to add more DNS servers, repeat the following procedure.

To set the DNS servers:

1. Select **5** from the main menu.
2. Select **1** to add a name server.
3. When prompted, enter the new nameserver in dotted decimal notation.

Change Time Options

You can change time zones or NTP configuration. The default time zone is set for (Pacific Standard Time (PST)/Pacific Daylight Time (PDT)). Select time zones in the following order:

- Continent or ocean
- Country
- Region

NOTE: NTP is disabled by default. We recommend that you enable this option to ensure that the time is always accurate.

To change time options:

1. Select **6** from the main menu.
2. Select **1** to change the time zone.

Follow the prompts to find the time zone you want based on the options listed earlier. The final selection returns you to the main menu.

3. Select **2** to set NTP servers.

NTP servers automatically set the system clock based on external time sources.

4. Select one of the following numbered options.

- **1** to enable or disable NTP.
- **2** to add an NTP server.

The remaining numbered options allow you to remove an NTP server from the list.

5. Follow the prompts to enable, set, or delete the NTP servers and return to the main menu.

Forward Local Status E-mails

You can use this option to forward all local root e-mails to an e-mail address. You can add an unlimited number of e-mail addresses in addition to mailing lists to help manage large numbers of recipients

To set the Forward Local Status:

1. Enter **7** from the main menu.
2. Enter **1** to add or change the recipient.
3. Enter **2** to remove the recipient.

System Security Update

System security updates are NSM*Xpress* operating system-level patches that protect the system against any future reported security vulnerabilities.

To manage system security updates:

1. Select **8** from the main menu.
2. Select one of the following options:
 - **1** to check for and install security updates now.
 - **2** to enable or disable automatic security updates.
 - **3** to check for and install the latest available NSM*Xpress* version.
 - **4** to set the proxy for security update check.
3. Follow the prompts to manage security updates, then return to the main menu.

Saving Setup Options

Before you configure the regional server or the central manager, NSM*Xpress* opens the Apply Change submenu. If you quit out of a menu after making changes, NSM*Xpress* also opens this screen and prompts you to save your changes. Updates are enabled by default. NSM*Xpress* checks for new updates daily by connecting to Juniper.

Figure 25: Saving Queued Changes

```

Select a change to cancel it:
1> IP Change: eth1 is 192.168.1.78 / 255.255.255.0
2> Add route: 192.168.0.0 / 255.255.0.0 -> eth1 : [192.168.1.254]
3> DNS add: 192.168.2.2
4> Enable NTP
5> Security updates: automatic check Disabled

A> Apply all changes
M> Make more changes
C> Cancel all changes and quit
R> Redraw menu

Choice [1-5,A,M,C,R]:

```

You have three options for saving changes:

- Select one of the following menu options:
 - **A** to apply all the new changes.
 - **M** to make more changes before configuring the regional server or the central manager.
 - **C** to cancel all new changes and quit the NSMXpress setup program. After canceling a change, the Change Apply submenu reappears.
- Select the number next to a displayed change to cancel only the selected change.
- Highlight one of the options you modified and delete it.

NSMXpress Default Restoration

When you re-install NSMXpress, you restore it to its factory defaults.

NOTE: NSMXpress is completely re-imaged by a re-install. No user data remains on the system. If you want to preserve your database, back it up before re-installing.

To re-install NSMXpress, use the following procedure. The steps in the procedure assume NSMXpress is connected to the computer running a null-modem cable. If not, refer to the section “Initial Setup Configuration” on page 6 for details.

To re-install the NSMXpress configuration:

1. Turn on NSMXpress.
2. Press any key while the Booting NSMXpress countdown scrolls through the screen to access the boot menu. See Figure 26.

Figure 26: Booting NSMXpress Countdown

```
Press any key to enter the menu

Booting NSMXpress
Booting NSMXpress
Booting NSMXpress
Booting NSMXpress
Booting NSMXpress
Booting NSMXpress
    in 4 seconds...
```

3. Use the arrow keys to select Re-Install, then press Enter. See Figure 27.

Figure 27: Re-Install Instructions

```
+-----+
| NSMXpress > |
| Rescue      |
| Re-Install  |
| Rescue Boot from Secondary Drive |
+-----+
```

4. Read the paragraph (as shown in Figure 28) then press Enter.

Figure 28: Re-Install Instructions

```
Booting "Re-Install"

Using this option will completely erase your appliance and load the factory
default image. No data recovery is possible after re-installing. To confirm
erase and re-install, type "erase" at the password prompt. To abort and boot
into Rescue mode, just hit <Enter> at the password prompt. Press any key.
```

5. Enter **erase** at the prompt to erase the disk. This will take a few minutes.

When done, you are prompted to reboot. See Figure 29.

Figure 29: Login Screen After Re-Installing NSMXpress

```
+-----+ Complete +-----+
|
| Congratulations, your Juniper NSMXpress Management Appliance 1.0
| i386 installation is complete.
|
| Remove any installation media (diskettes or CD-ROMs) used during
| the installation process and press <Enter> to reboot your system.
|
|                                     +-----+
|                                     | Reboot |
|                                     +-----+
|
+-----+
```

6. Press Enter to reboot.

Chapter 3

Configuring NSM from the Web Interface

This chapter describes how to configure NSM from the NSM*Xpress* Web interface. It contains the following sections:

- Configuring the NSM Software on page 28
- Managing NSM Administration on page 35
- Managing System Administration on page 40
- Maintenance on page 43
- Troubleshooting on page 45

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 between a regional server and a central manger. All exceptions are noted.

For more information on how to use NSMXpress and configuration options, go to the following sections:

- Managing NSM Administration on page 35
- Managing System Administration on page 40
- Maintenance on page 43
- Troubleshooting on page 45

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

- Basic Settings, on page 28, for the minimum installation requirements.
- Advanced Options, on page 30, for additional installation options.

Basic Settings

To install the regional server software using the minimum requirements:

1. Complete all appropriate steps in Chapter 1, "Getting Started."
2. Enter the **https:// < ip > /admin** URL for your appliance in a Web browser. See "Web Interface Configuration," on page 8 for details.
3. Log into the Web interface as an 'admin' user to open the NSM Regional Server window (see Figure 30) or the NSM Central Manager window (see Figure 31).

NOTE: The 'admin' user default username is **admin** and the password is the one you created in Step 6 on page 6.

Figure 30: Regional Server Configuration Main Menu

Juniper NETWORKS NSM Xpress 2007.3r1

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 172.24.68.111
 The IP address on this server that will be used for management

NSM 'super' password
 Password for 'super' user

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

Remote Replication of Database Off Menu

High Availability Off Menu

SRS Off Menu

Submit

Install

Figure 31: Central Manager Configuration Main Menu

Juniper NETWORKS NSM Xpress 2007.3r1

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 172.24.68.111
 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

Submit

Install

4. 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 once you click the second radio button.

5. Enter the 'super' user password in the top text box, and then re-enter it in the text box below it.

This password must be at least eight characters long. There are no other requirements, however, this password is case sensitive. This password is used by the NSM 'super' user (also referred to as the NSM administrator). This user has the highest level of privileges in NSM.

6. 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 enable **Browse**. This allows you 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.
7. Click **Submit** to save any changes and then click **Install** to install the software.

Advanced Options

All advanced installation options are optional.

- **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.
- **High Availability**—Opens a menu to help you configure HA.
- **SRS Enabled Options**—Opens a menu to help configure Statistical Report Server (SRS). These options enable NSMExpress to interface with SRS. You can toggle it on or off. When it is on, a menu with additional options are available.

NOTE: Juniper SRS is a complementary product to NSM and must be installed on a separate server.

Remote Replication of Database

To configure remote replication of database settings:

1. Click **Menu** next to Remote Replication of Database (see Figure 32) to configure daily backups (see Figure 33).

Figure 32: Remote Replication of Database Menu Option

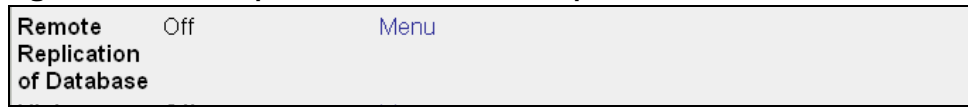
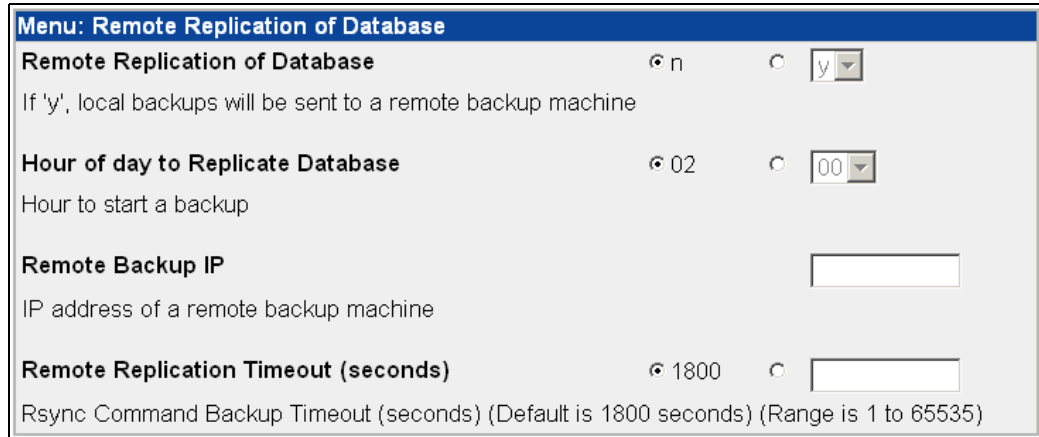


Figure 33: Remote Replication of Database Options



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 machine.

Backup information is copied to the /var/netscreen/dbbackup directory on the remote server. The 'nsm' user must exist on both machines and you must establish an SSH trust relationship. See the *NetScreen-Security Manager Installer 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.

High Availability

To configure high availability (HA) settings:

1. Click **Menu** next to High Availability to access HA options. See Figure 34.

Figure 34: High Availability Options

Menu: High Availability	
High Availability	<input type="radio"/> n <input checked="" type="radio"/> y
Whether to enable HA on this server or not	
Primary Status	<input type="button" value="y"/>
If 'y', this machine is a Primary Server and if 'n' this machine is a Secondary Server	
HA Remote IP	<input type="text"/>
IP address for the peer's primary heartbeat link	
HA Link Failure Detection IP	<input type="text"/>
IP address outside the HA cluster	
HA Inter-server password	<input type="text"/>
Shared password for heartbeat	
Shared Disk	Off Menu
HA Links	Menu
HA Advanced Settings	Menu

- Use the High Availability option to turn HA on (**y**) or off (**n**). The default is off.
- Use the Primary Status option to set your NSMExpress 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.
- Use the HA Remote IP option to enter the IP address for the HA peer in the HA cluster.
- Use the HA Link Failure Detection IP option to enter the IP address of a machine outside of the HA cluster that you can ping to verify connection status.
- Use the HA Inter-server password option to enter the heartbeat password used between the primary and secondary servers.
- Click **Submit** to save the changes.
- Click **Menu** next to Shared Disk (see Figure 34) to configure a shared disk for regional servers (see Figure 35) or for central managers (see Figure 36). This step is optional.

Figure 35: Shared Disk Options for Regional Servers

Menu: Shared Disk

Shared Disk: Gui Server n y
If 'y', data directory for GUI Server is a shared disk partition

Shared Disk: Device Server n y
If 'y', data directory for Device Server is a shared disk partition

Shared Disk Source (NFS)
Source of shared disk, e.g. /dev/sdc1 or server:/share

Shared Disk NFS Mount Options rw r
Options when mounting shared disk e.g. rw,intr,tcp,soft,timeo

Figure 36: Shared Disk Options

Menu: Shared Disk

Shared Disk: Gui Server
If 'y', data directory for GUI Server is a shared disk partition

Shared Disk Source (NFS)
Source of shared disk, e.g. /dev/sdc1 or server:/share

Shared Disk NFS Mount Options
Options when mounting shared disk e.g. rw,intr,tcp,soft,timeo

NSM*Xpress* supports shared disk via NFS only. Due to the data-intensive nature of NSM, gigabit speed links (1000 Mbps) are highly recommended for Shared Disk usage. For more information on options available to you for custom settings, refer to the *NetScreen-Security Manager Installer Guide*.

9. Click **Menu** next to HA Links (see Figure 34) to configure the second link in the HA cluster (see Figure 37). This step is optional.

Figure 37: HA Links Options

Menu: HA Links

HA Link count 1 2
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. Setting a redundant link is optional. For more information on options available to you for custom settings, refer to the *NetScreen-Security Manager Installer Guide*.

10. Click **Menu** next to the HA Advanced Settings (see Figure 34) to configure HA advanced setting (see Figure 38). This step is optional.

For more information on options available to you for custom settings, refer to the *NetScreen-Security Manager Installer Guide*.

Figure 38: HA Advanced Settings

Menu: HA Advanced Settings		
HA Heartbeat Frequency	<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)		
HA Heartbeat Failure Threshold	<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)		
HA Data Replication Timeout	<input checked="" type="radio"/> 1800	<input type="radio"/> <input type="text"/>
Rsync Command Replication Timeout (Default is 1800 seconds) (Range is 1 to 65535)		

11. Click **Submit** to save the HA options and return to the NSM Configuration Main Menu or continue with the following HA options and then click **Submit** to save the options and return to the NSM Configuration Main Menu:

- Shared Disk
- HA Links
- HA Advanced Settings

SRS Enabled Options

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

1. Click **Menu** next to SRS (see Figure 34) to open the SRS menu (see Figure 39).

Figure 39: SRS Menu

Menu: SRS		
SRS	<input checked="" type="radio"/> n	<input type="radio"/> <input type="text" value="y"/>
Statistical Report Server will be used with this GUI Server		
SRS DB IP		<input type="text"/>
Database server IP address		
SRS DB Type	<input checked="" type="radio"/> postgresql	<input type="radio"/> <input type="text" value="postgresql"/>
Database type		
SRS Database Name	<input checked="" type="radio"/> netscreen	<input type="radio"/> <input type="text"/>
Database name		
SRS DB Owner Name	<input checked="" type="radio"/> netscreen	<input type="radio"/> <input type="text"/>
Database user name		
SRS DB Owner Password		<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. Re-enter it in the second text box.
8. Click **Submit** to save the options and return to the NSM Configuration Main Menu.

Install NSM Software

Once you submit all your configuration options, click **Install** to install the NSM software on your NSM*Xpress* appliance. This will take a few minutes. Note the status ball in the navigation tree moving from left to right to indicate installation is progressing. Wait for the status ball to stop before continuing to use the Web interface.

For more information on how to use NSM*Xpress* and configuration options, go to the following sections:

- Managing NSM Administration on page 35
- Managing System Administration on page 40
- Maintenance on page 43
- Troubleshooting on page 45

Managing NSM Administration

Use the options in the NSM Administration section to:

- Change the Superuser Password
- Download NSM MIBS
- Export Audit Logs
- Export Device Logs

- Generate Reports
- Modify NSM Configuration Files
- Back Up the NSM Database
- Change the NSM Management IP
- Schedule Security Updates

Change the Superuser Password

To change the super user password, click the NSM Super User Password link under NSM Administration to change this password. See Figure 40.

Figure 40: Change Super User Password

The screenshot shows a web form titled "Change Password for Super User". It contains two text input fields: "Password:" and "Confirm Password:". Below the fields are two buttons: "Change Super User Password" and "Clear".

Download NSM MIBS

Use this option to download any available MIBs (see Figure 41). This option is not available on central manager.

Figure 41: Download NSM MIBS

The screenshot shows a web form titled "Download NSM MIBS". It contains a single button labeled "Download MIB".

Export Audit Logs

Use this option to export audit logs. To export an audit log to a cvs file, select cvs in the drop-down list box, then enter the cvs file name in the text box below it. See Figure 42.

Figure 42: Export Audit Logs

The screenshot shows a web form titled "Export Audit Logs". It features a "Select Export Type:" label above a dropdown menu currently set to "CSV". Below the dropdown is a text input field. Underneath the field is the text "Enter cvs file-name". At the bottom of the form is a button labeled "Export Audit Logs".

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

Export Device Logs

Use this option to export device logs (see Figure 43). This option is not available on central manager.

Figure 43: Export Device Logs

Export Device Logs

Select Filter:

category

Enter category

Select Action:

XML

Enter xml file name

Enter include-header(optional)

Export Device Logs

Generate Reports

Use this option to generate reports (see Figure 44). This option is not available on central manager.

Figure 44: 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:

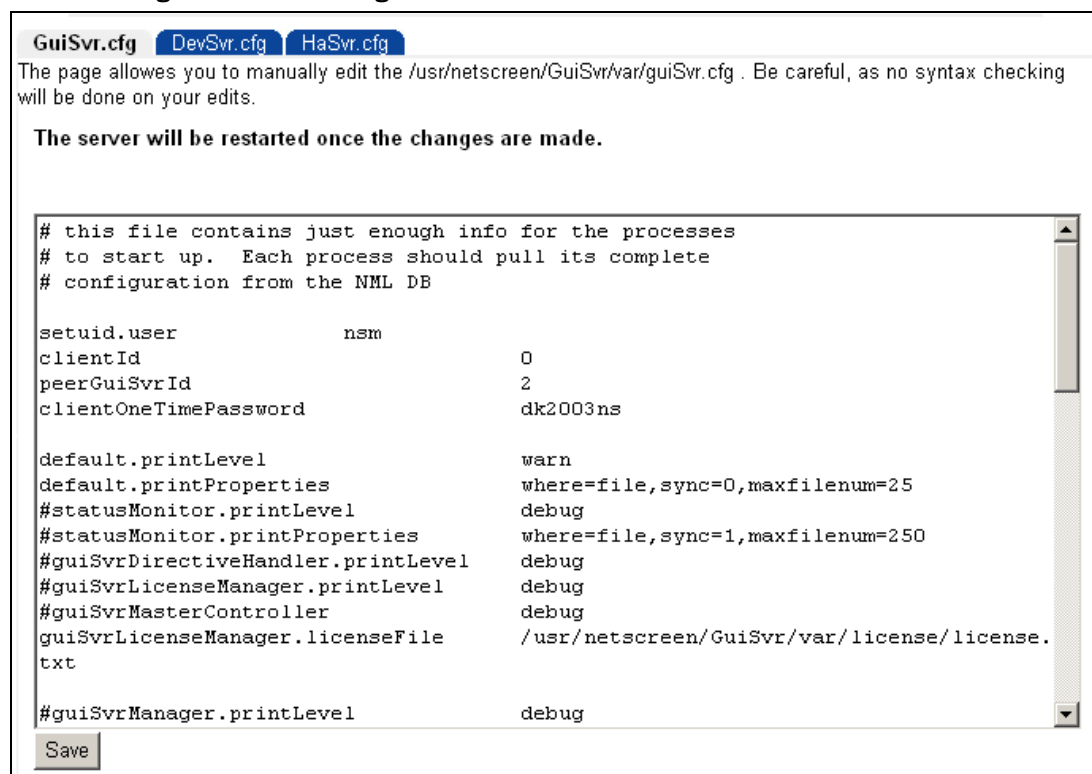
Generate Reports

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

Modify NSM Configuration Files

Use the windows in the NSM Configuration Files option to manually edit the GuiSvr.cfg, DevSrv.cfg, and HaSvr.cfg files. The example, in Figure 45, shows the option to modify the GuiSvr.cfg file.

Figure 45: NSM Configuration Files



NSM Database Backup

To back up the NSM database file, click the NSM Database Backup link under NSM Administration. See Figure 46.

Figure 46: Database Backup

NSM Backup Configuration Parameters

Local Backup Enabled y

Remote Backup enabled n

Hour of Day to Replicate Database 02

Remote Backup IP

Submit

Execute Backup Now

Apply

Download Database Backup Files

File to Download ...

Change the NSM Management IP

To change the IP address of the NSM management server, click the NSM Management IP link under NSM Administration. See Figure 47.

Figure 47: Change Management IP

NSM Management IP

Management Ip 172.24.68.111

Schedule Security Updates

To schedule security updates. See Figure 48.

Figure 48: Schedule Security Updates

Security Update

Select Post Action:

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

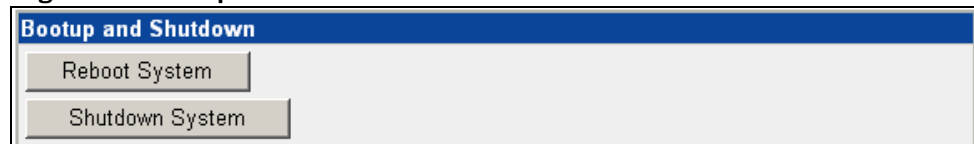
Use the options in the NSM Administration section to:

- Reboot and shut down
- Change the user password
- Configure the network
- Change the system time
- Install updates
- Configure the Web Interface

Reboot and Shut Down

To reboot or shut down NSMXpress, click the **Reboot System** and **Shutdown System** buttons (see Figure 49) after selecting the reboot option under System Administration.

Figure 49: Boot Up and Shut Down



Change the User Password

To change the user password, click **Change User Password** under System Administration. Fill out the form and then click **Change**. See Figure 50.

Figure 50: Change User Password

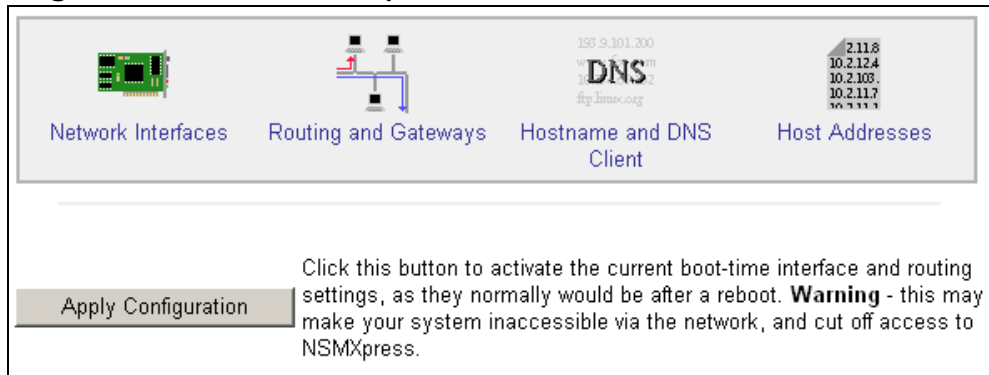
 A screenshot of a web interface window titled "Changing NSMXpress user password". The window has a blue header bar with the title. Below the header, there is a form with the following elements:

- "Changing password for" with the value "admin" displayed next to it.
- "Old password" with an empty text input field.
- "New password" with an empty text input field.
- "New password (again)" with an empty text input field.
- At the bottom, there are two buttons: "Clear form" and "Change".

Configure the Network

To access options that allow you to configure the network, click **Network Configuration** under System Administration to open the network options window. See Figure 51.

Figure 51: Network Interfaces Options



Network interfaces

Use this option to manage the network interfaces. See Figure 52.

Figure 52: 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

Routes and Gateways

Use this option to configure and manage routes and gateways. See Figure 53.

Figure 53: 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 54.

Figure 54: DNS Client Options

DNS Client Options

Hostname: NSMXpress.juniper.net

Resolution order: Hosts, DNS, [], [], []

Update hostname in host addresses if changed?

DNS servers: [], [], []

Search domains: None Listed ..

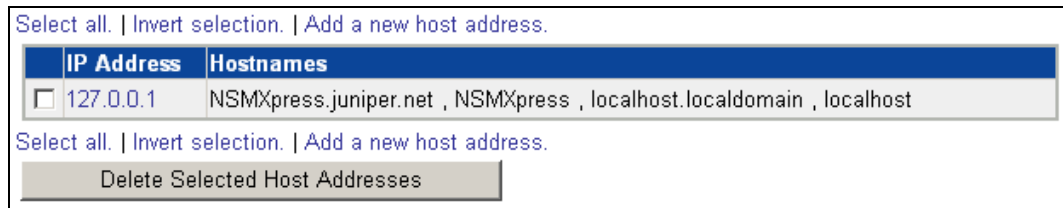
juniper.net

Save

Host addresses

Use this option to manage host addresses, See Figure 55.

Figure 55: Host Address



System Time

Use this option to change the system time and time zones.

System Updates

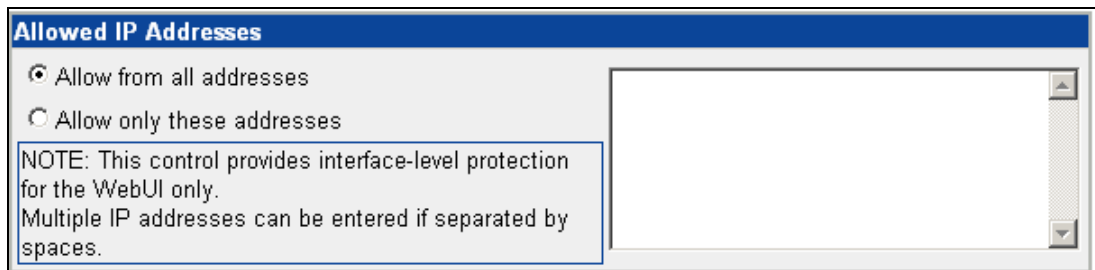
Use this option to:

- 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.

Configure the Web Interface

Use this option to provide interface-level protection for the Web interface. See Figure 56.

Figure 56: Web Interface Access



Maintenance

To view system statistics, select the Maintenance option and click System Statistics.

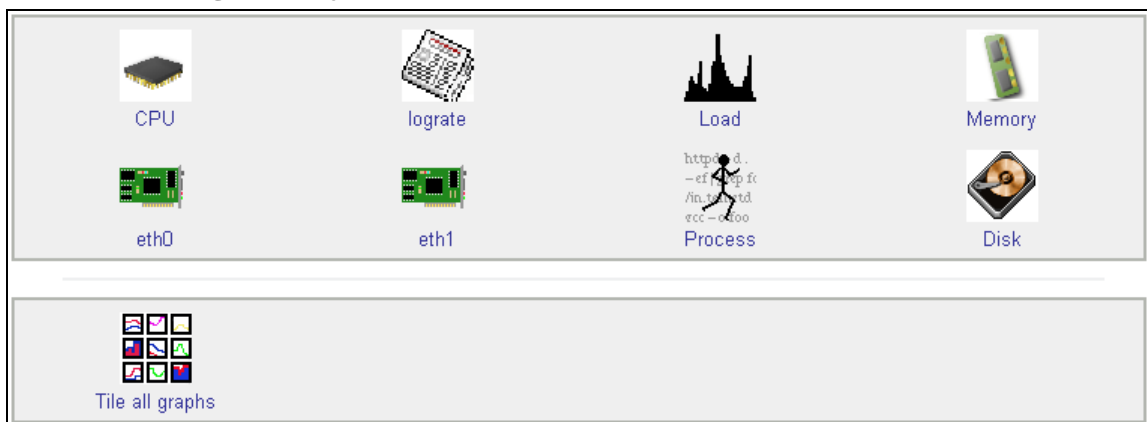
System Statistics

Use the options in the Maintenance section (see Figure 57) to view the following system statistics:

- CPU
- Log rate

- Load
- Memory
- Interfaces
- Process count
- Disk
- Tile All Graphs

Figure 57: System Statistics



CPU

Use this option to view graphs that monitor the CPU activity on an hourly, daily, weekly, monthly or on a customizable basis.

Log Rate

Use this option to view graphs that monitor the log rate on an hourly, daily, weekly, monthly or on a customizable basis.

CPU Load

Use this option to view graphs that monitor the CPU load on an hourly, daily, weekly, monthly or on a customizable basis.

Memory Data

Use this option to view graphs that monitor the memory activity on an hourly, daily, weekly, and monthly basis.

Network Data

Select either eth0 or eth1 to view graphs that monitor network activity on an hourly, daily, weekly, and monthly basis.

Process Count

Use this option to view graphs that monitor the number of processes on an hourly, daily, weekly, and monthly basis.

Disk Data

Use this option to view graphs that monitor the file system disk space usage on an hourly, daily, weekly, and monthly basis.

Tile All Graphs

Use this option 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:

- Error logs
- Network utilities
- Tech Support

Error Logs

To review your error log (see Figure 58), click **Error Logs** under Troubleshooting.

Figure 58: Review Error Logs

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

To view details of an individual error log, select the file you want to view and click **View**. See Figure 59.

Figure 59: Error Log Detail

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

The Network Utilities provide basic tools (ping, traceroute and nslookup) for TCP/IP Networking. It also provides an IP subnet calculator. Use it to calculate a netmask by

Network Class and number or by number of hosts. The calculation shows the smallest subnet available. See Figure 60.

Figure 60: Network Utilities Options



Ping

Ping is a tool for checking network connectivity. NSMExpress prompts with the following questions so you can focus your search. See Figure 61.

- How many packets?
- Packet size?
- How many sec between sending each packet?
- Pattern(s) to send (Hex)?
- Verbosity output?
- Numeric output only?
- Bypass routing tables?

Figure 61: Ping Utility

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)?

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

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 packets.

Pattern(s) to Send (Hex)

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

Verbosity Output

NSM*Xpress* 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 62.

Figure 62: Traceroute Utility

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

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 63). 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 NSM*Xpress* is installed. nslookup will use this time (in seconds) to stop the lookup if it does not get an answer for this amount.

Figure 63: Lookup Utility

Hostname	<input type="text"/>
Type:	<input type="text" value="Network address (A)"/>
Nameserver:	<input type="radio"/> Default <input checked="" type="radio"/> <input type="text"/>
Timeout?	<input type="text" value="10"/>
<input type="button" value="Look Up!"/>	

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 you can calculate a netmask by the number of hosts (see Figure 64). When you calculate a netmask by the number of hosts, NSMExpress returns the smallest network available.

Figure 64: IP Subnet Calculator

Calculate Netmask by Class and Bits			
Class:	<input type="text" value="C (192.x.x.x-223.x.x.x)"/>	Subnet Bits: <input type="text" value="0"/>	<input type="button" value="Calculate Subnet"/>
Calculate Netmask by Number of Hosts			
Number of Hosts:	<input type="text"/>	<input type="button" value="Calculate Subnet"/>	

Tech Support

To get contact information for Juniper Tech Support, click **Tech Support** under Troubleshooting. To help analyze problems, select a detail type in the drop-down list box, then click **Run Tech-Support Script**. NSMExpress creates a file you can download and send to Juniper Tech Support. See Figure 65.

Figure 65: Juniper Tech Support

Tech Support	
<input type="text" value="Details from Gui, Device and HA servers"/>	
<input type="button" value="Run Tech-Support Script"/>	
JTAC WEBSITE: https://support.juniper.net	
JTAC PHONE NUMBER: 1-888-314-JTAC	
JTAC FTP SITE: ftp.juniper.net	