END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT (“AGREEMENT”) BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. The Parties. The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer’s principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer’s principal office is located outside the Americas) (such applicable entity being referred to herein as “Juniper”), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software (“Customer”) (collectively, the “Parties”).

2. The Software. In this Agreement, “Software” means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. “Software” also includes updates, upgrades and new releases of such software. “Embedded Software” means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. License Grant. Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees, provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer’s use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer’s use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

d. For any trial copy of the Software, Customer’s right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer’s enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. Use Prohibitions. Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any “locked” or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller, (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. Audit. Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.
6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer’s internal business purposes.

7. **Ownership.** Juniper and Juniper’s licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the “Warranty Statement”). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper’s or its suppliers’ or licensors’ liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer’s possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer’s payment of any withholding taxes, completing appropriate applications that would reduce the amount of withholding tax to be paid, and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Juniper will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer’s non-compliance with the applicable tax laws and regulations. Customer’s obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer’s ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is “commercial computer software” and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT II); as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer’s written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License (“GPL”) or the GNU Library General Public License (“LGPL”)), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at http://www.gnu.org/licenses/gpl.html, and a copy of the LGPL at http://www.gnu.org/licenses/lgpl.html.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous
agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentiés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui y rattaché, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language).)
Table of Contents

About This Guide xv

Objectives ......................................................................................................xv
Audience .......................................................................................................xv
Conventions ..................................................................................................xv
Documentation ............................................................................................xvii
Documentation Feedback ...........................................................................xviii
Requesting Technical Support .....................................................................xviii

Part 1

Using NSMXpress

Chapter 1  Getting Started 3

About NSMXpress ...........................................................................................3
Installation and Configuration Workflow ...................................................4
Hardware Installation ......................................................................................4
NSMXpress Ports ......................................................................................4
Installing the Hardware .............................................................................5
Initial Setup Configuration ...............................................................................7
Boot NSMXpress .......................................................................................7
Set Up Your Appliance ..............................................................................8
CLI Configuration ...............................................................................8
Web Interface Configuration ........................................................................9

Chapter 2  Installing and Configuring NSM from the CLI 11

Navigating the Menus ....................................................................................11
General Options ...........................................................................................11
Using nsm_setup ....................................................................................12
Configuring the NSM Software ..............................................................13
Configuring a Regional Server ..................................................................14
Configuring Typical Settings ........................................................................14
Configuring Custom Settings ......................................................................15
   Configuring High Availability ..............................................................16
   Configuring Advanced Options .........................................................17
Configuring the Central Manager ............................................................19
   Configuring High Availability ..............................................................21
   Configuring Advanced Options .........................................................25
      Enabling and Configuring Remote Replication of the Database ......25
### Configuring Standard Configuration Options
- Changing the Password .................................................24
- Setting Interface Options .............................................24
- Setting Routing Options ...............................................24
- Changing the NSMXpress Hostname .................................25
- Adding DNS Servers ....................................................25
- Setting the System Time ...............................................26
- Forwarding Local Status E-mails .....................................26
- Updating System Security .............................................26
- Saving Setup Options ..................................................27
- NSMXpress Default Restoration .................................28

### Chapter 3 Configuring NSM from the Web Interface

#### Configuring NSM from the Web Interface
- Configuring the NSM Software ...................................31
- Configuring Basic Settings ........................................31
- Configuring High Availability .....................................34
- Advanced Options ..................................................36
- Enabling and Configuring Remote Replication of the Database 37
- Enabling and Configuring SRS (Regional Server Only) ....38
- Installing NSM Software ...........................................39
- Managing NSM Administration ..................................40
- Changing the Superuser Password ............................40
- Downloading NSM MIBS (Regional Server Only) .........40
- Exporting Audit Logs ...............................................41
- Exporting Device Logs (Regional Server Only) ..............41
- Generating Reports (Regional Server Only) ..................42
- Modifying NSM Configuration Files .........................42
- Backing Up the NSM Database ..................................43
- Changing the NSM Management IP .........................44
- Scheduling Security Updates .....................................44
- Managing System Administration .............................45
- Rebooting or Shutting Down NSMXpress ...................45
- Changing the User Password .....................................45
- Configuring the Network ...........................................46
- Network Interfaces .................................................47
- Routing and Gateways ............................................47
- Hostname and DNS Clients .......................................48
- Host Addresses .....................................................48
- Monitoring with SNMP ...........................................49
- SNMP Configuration ...............................................49
- SNMP System Information .................................50
- SNMP Trap Configuration ........................................50
- Forwarding Syslog Messages .................................51
- Viewing Syslog Receivers .......................................52
- Adding and Configuring Syslog Receivers .................53
- Editing Syslog Receiver Configurations ..................55
- Deleting Syslog Receivers ......................................55
- Changing the System Time ......................................55
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing Updates</td>
<td>56</td>
</tr>
<tr>
<td>Configuring the Web Interface</td>
<td>56</td>
</tr>
<tr>
<td>Maintaining NSMXpress</td>
<td>56</td>
</tr>
<tr>
<td>Viewing System Statistics</td>
<td>56</td>
</tr>
<tr>
<td>CPU</td>
<td>57</td>
</tr>
<tr>
<td>Log Rate</td>
<td>57</td>
</tr>
<tr>
<td>CPU Load</td>
<td>57</td>
</tr>
<tr>
<td>Memory Data</td>
<td>57</td>
</tr>
<tr>
<td>Network Data</td>
<td>57</td>
</tr>
<tr>
<td>Process Count</td>
<td>57</td>
</tr>
<tr>
<td>Disk Data</td>
<td>57</td>
</tr>
<tr>
<td>Tile All Graphs</td>
<td>58</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>58</td>
</tr>
<tr>
<td>Error Logs</td>
<td>58</td>
</tr>
<tr>
<td>Network Utilities</td>
<td>59</td>
</tr>
<tr>
<td>Ping</td>
<td>59</td>
</tr>
<tr>
<td>Traceroute</td>
<td>60</td>
</tr>
<tr>
<td>Lookup</td>
<td>61</td>
</tr>
<tr>
<td>IP Subnet Calculator</td>
<td>61</td>
</tr>
<tr>
<td>Tech Support</td>
<td>61</td>
</tr>
<tr>
<td>Viewing System Information</td>
<td>62</td>
</tr>
</tbody>
</table>

**Part 2**

**Appendixes**

**Appendix A**

**NSMXpress LEDs**

NSMXpress LEDs ...........................................................................................65

**Part 3**

**Index**

Index .............................................................................................................69
List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Front Panel of NSMXpress</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>Regional Server Configuration Main Menu</td>
<td>32</td>
</tr>
<tr>
<td>3</td>
<td>Central Manager Configuration Main Menu</td>
<td>33</td>
</tr>
<tr>
<td>4</td>
<td>High Availability Options</td>
<td>34</td>
</tr>
<tr>
<td>5</td>
<td>Shared Disk Options for Regional Servers</td>
<td>35</td>
</tr>
<tr>
<td>6</td>
<td>Shared Disk Options for Central Managers</td>
<td>35</td>
</tr>
<tr>
<td>7</td>
<td>HA Links Options</td>
<td>35</td>
</tr>
<tr>
<td>8</td>
<td>Redundant Links</td>
<td>36</td>
</tr>
<tr>
<td>9</td>
<td>HA Advanced Settings</td>
<td>36</td>
</tr>
<tr>
<td>10</td>
<td>Advanced Options Menu</td>
<td>37</td>
</tr>
<tr>
<td>11</td>
<td>Remote Replication of Database Options</td>
<td>38</td>
</tr>
<tr>
<td>12</td>
<td>SRS Menu</td>
<td>39</td>
</tr>
<tr>
<td>13</td>
<td>Change Superuser Password</td>
<td>40</td>
</tr>
<tr>
<td>14</td>
<td>Download NSM MIBs</td>
<td>41</td>
</tr>
<tr>
<td>15</td>
<td>Export Audit Logs</td>
<td>41</td>
</tr>
<tr>
<td>16</td>
<td>Export Device Logs</td>
<td>41</td>
</tr>
<tr>
<td>17</td>
<td>Generate Reports</td>
<td>42</td>
</tr>
<tr>
<td>18</td>
<td>NSM Configuration Files</td>
<td>43</td>
</tr>
<tr>
<td>19</td>
<td>Database Backup</td>
<td>44</td>
</tr>
<tr>
<td>20</td>
<td>Change Management IP</td>
<td>44</td>
</tr>
<tr>
<td>21</td>
<td>Schedule Security Updates</td>
<td>45</td>
</tr>
<tr>
<td>22</td>
<td>Boot Up and Shut Down</td>
<td>45</td>
</tr>
<tr>
<td>23</td>
<td>Change User Password</td>
<td>46</td>
</tr>
<tr>
<td>24</td>
<td>Network Interfaces Options</td>
<td>46</td>
</tr>
<tr>
<td>25</td>
<td>Network Interfaces</td>
<td>47</td>
</tr>
<tr>
<td>26</td>
<td>Routes and Gateways</td>
<td>48</td>
</tr>
<tr>
<td>27</td>
<td>DNS Client Options</td>
<td>48</td>
</tr>
<tr>
<td>28</td>
<td>Host Address</td>
<td>48</td>
</tr>
<tr>
<td>29</td>
<td>Configuring SNMP</td>
<td>49</td>
</tr>
<tr>
<td>30</td>
<td>Configuring SNMP System Information</td>
<td>50</td>
</tr>
<tr>
<td>31</td>
<td>Configuring SNMP Traps</td>
<td>51</td>
</tr>
<tr>
<td>32</td>
<td>Configuring a Syslog Receiver</td>
<td>54</td>
</tr>
<tr>
<td>33</td>
<td>Web Interface Access</td>
<td>56</td>
</tr>
<tr>
<td>34</td>
<td>System Statistics</td>
<td>57</td>
</tr>
<tr>
<td>35</td>
<td>Review Error Logs</td>
<td>58</td>
</tr>
<tr>
<td>36</td>
<td>Error Log Detail</td>
<td>58</td>
</tr>
<tr>
<td>37</td>
<td>Network Utilities Options</td>
<td>59</td>
</tr>
<tr>
<td>38</td>
<td>Ping Utility</td>
<td>59</td>
</tr>
<tr>
<td>39</td>
<td>Traceroute Utility</td>
<td>60</td>
</tr>
<tr>
<td>40</td>
<td>Lookup Utility</td>
<td>61</td>
</tr>
<tr>
<td>41</td>
<td>IP Subnet Calculator</td>
<td>61</td>
</tr>
<tr>
<td>42</td>
<td>Juniper Tech Support</td>
<td>62</td>
</tr>
</tbody>
</table>
List of Tables

Table 1: Notice Icons .................................................................xvi
Table 2: Text Conventions ...........................................................xvi
Table 3: Syntax Conventions .........................................................xvii
Table 4: Network and Security Manager Publications ..................xvii
Table 5: Required Ports on NSMXpress .................................5
Table 6: Ethernet Port LEDs .........................................................7
Table 7: Viewing Syslog Receivers ...........................................52
Table 8: NSMXpress LEDs ..........................................................65
About This Guide

About This Guide contains the following sections:

- Objectives on page xv
- Audience on page xv
- Conventions on page xv
- Documentation on page xvii
- Documentation Feedback on page xviii
- Requesting Technical Support on page xviii

Objectives

Juniper Networks NSMXpress is an appliance version of Network and Security Manager (NSM), a software application that centralizes control and management of your Juniper Networks devices. With NSM, Juniper Networks delivers integrated, policy-based security and network management for network and security devices. NSMXpress runs NSM 2008.2.

NSMXpress simplifies the complexity of device administration by providing a single, integrated management interface that controls device parameters. 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 NSMXpress command-line interface (CLI) or the Web interface.

Audience

This guide is intended for system administrators responsible for the security infrastructure of their organization. Specifically, this book provides procedures for firewall and VPN administrators, network/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 software. The actual screens may differ.
All examples show default file paths. If you do not accept the installation defaults, your paths will vary from the examples.

Table 1 on page xvi defines notice icons used in this guide.

### Table 1: Notice Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📝</td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td>🔴</td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td>⚥️</td>
<td>Laser warning</td>
<td>Alerts you to the risk of personal injury from a laser.</td>
</tr>
</tbody>
</table>

Table 2 on page xvi defines text conventions used in this guide.

### Table 2: Text Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold typeface like this</strong></td>
<td>Represents commands and keywords in text.</td>
<td>Issue the <strong>clock source</strong> command.</td>
</tr>
<tr>
<td></td>
<td>Represents keywords</td>
<td>Specify the keyword <strong>exp-msg</strong></td>
</tr>
<tr>
<td></td>
<td>Represents UI elements</td>
<td>Click <strong>User Objects</strong></td>
</tr>
<tr>
<td><strong>Bold typeface like this</strong></td>
<td>Represents text that the user must type.</td>
<td>user input</td>
</tr>
<tr>
<td><strong>fixed-width font</strong></td>
<td>Represents information as displayed on the terminal screen.</td>
<td><strong>host1# show ip ospf</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Routing Process OSPF 2 with Router ID 5.5.0.250</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Router is an area Border Router (ABR)</td>
</tr>
<tr>
<td><strong>Key names linked with a plus ( + ) sign</strong></td>
<td>Indicates that you must press two or more keys simultaneously.</td>
<td>Ctrl + d</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>Emphasizes words</td>
<td>The product supports two levels of access, <strong>user</strong> and <strong>privileged</strong>.</td>
</tr>
<tr>
<td></td>
<td>Identifies variables</td>
<td><strong>clusterID</strong>, <strong>ipAddress</strong></td>
</tr>
<tr>
<td><strong>The angle bracket ( &gt; )</strong></td>
<td>Indicates navigation paths through the UI by clicking menu options and links.</td>
<td><strong>Object Manager</strong> &gt; <strong>User Objects</strong> &gt; <strong>Local Objects</strong></td>
</tr>
</tbody>
</table>
Table 3 on page xvii defines syntax conventions used in this guide.

**Table 3: Syntax Conventions**

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Words in plain text</td>
<td>Represent keywords</td>
<td>terminal length</td>
</tr>
<tr>
<td>Words in italics</td>
<td>Represent variables</td>
<td>mask, accessListName</td>
</tr>
<tr>
<td>Words separated by the pipe (</td>
<td>) symbol</td>
<td>Represent a choice to select one keyword or variable to the left or right of this symbol. The keyword or variable can be optional or required.</td>
</tr>
<tr>
<td>Words enclosed in brackets ( [ ] )</td>
<td>Represent optional keywords or variables.</td>
<td>[ internal</td>
</tr>
<tr>
<td>Words enclosed in brackets followed by and asterisk ( [ ])*</td>
<td>Represent optional keywords or variables that can be entered more than once.</td>
<td>[ level1</td>
</tr>
<tr>
<td>Words enclosed in braces ( { } )</td>
<td>Represent required keywords or variables.</td>
<td>{ permit</td>
</tr>
</tbody>
</table>

**Documentation**

Table 4 on page xvii describes documentation for NSM.

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

<table>
<thead>
<tr>
<th>Book</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Network and Security Manager Installation Guide</em></td>
<td>Describes the steps to install the NSM management system on a single server or on separate servers. It also includes information on how to install and run the NSM user interface. This guide is intended for IT administrators responsible for the installation or upgrade of NSM.</td>
</tr>
<tr>
<td><em>Network and Security Manager Administration Guide</em></td>
<td>Describes how to use and configure key management features in the NSM. It provides conceptual information, suggested workflows, and examples. This guide is best used in conjunction with the NSM Online Help, which provides step-by-step instructions for performing management tasks in the NSM UI. This guide is intended for application administrators or those individuals responsible for owning the server and security infrastructure and configuring the product for multiuser systems. It is also intended for device configuration administrators, firewall and VPN administrators, and network security operation center administrators.</td>
</tr>
<tr>
<td><em>Network and Security Manager Configuring ScreenOS and IDP Devices Guide</em></td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 4: Network and Security Manager Publications (continued)

<table>
<thead>
<tr>
<th>Book</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network and Security Manager Online Help</td>
<td>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.</td>
</tr>
<tr>
<td>Network and Security Manager API Guide</td>
<td>Provides complete syntax and description of the SOAP messaging interface to NSM.</td>
</tr>
<tr>
<td>Network and Security Manager Release Notes</td>
<td>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.</td>
</tr>
<tr>
<td>NSMXpress User Guide</td>
<td>Describes how to set up and manage the NSMXpress appliance as a central manager or regional server.</td>
</tr>
</tbody>
</table>

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version (not required for Network Operations Guides [NOGs])

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 postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at http://www.juniper.net/customers/support/downloads/710059.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.
Self-Help Online Tools and Resources

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

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

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

**Opening a Case with JTAC**

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

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

For international or direct-dial options in countries without toll-free numbers, visit us at [http://www.juniper.net/support/requesting-support.html](http://www.juniper.net/support/requesting-support.html).
Requesting Technical Support
Part 1

Using NSMXpress

Part 1 contains the following chapters:

- Getting Started on page 3
- Installing and Configuring NSM from the CLI on page 11
- Configuring NSM from the Web Interface on page 31
Chapter 1
Getting Started

This version of NSM Xpress comes preconfigured as a regional server or central manager.

This chapter contains the following sections:
■ About NSM Xpress on page 3
■ Hardware Installation on page 4
■ Initial Setup Configuration on page 7

About NSM Xpress

NSM Xpress is an appliance version of Network and Security Manager (NSM) and runs NSM 2008.2. NSM Xpress 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 NSM Xpress by eliminating the need to have dedicated resources for maintaining a network and security management solution.

NSM Xpress makes it easy for administrators to control device configuration, network settings, and security policy settings for multiple families of Juniper Networks devices including:
■ ScreenOS firewall/VPN devices and intrusion detection and prevention (IDP) devices
■ JUNOS devices, such as J-series routers, SRX-series gateways, EX-series switches, M-series Internet routers, and MX-series Ethernet Services routers.
■ Secure Access devices
■ Unified Access Control (Infranet Controller) devices.

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

Up to 10 administrators can log into NSM Xpress concurrently.
**Installation and Configuration Workflow**

This guide explains the steps for installing and configuring NSMXpress and for configuring NSM.

1. Install the NSMXpress appliance hardware.
2. Set up the NSMXpress appliance, using the serial port.
3. Configure the NSMXpress software, using either the CLI or the Web interface.
4. Configure NSM software, which was preinstalled 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.

**NSMXPRESS Ports**

Table 5 on page 5 provides required port information on the NSMXPRESS.
### Table 5: Required Ports on NSMXpress

<table>
<thead>
<tr>
<th>Direction</th>
<th>Port</th>
<th>Description</th>
<th>LAN</th>
<th>Internet</th>
<th>Depends on Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>In</td>
<td>22</td>
<td>SSH command-line management</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>443</td>
<td>Web interface for administrator login</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>8443</td>
<td>Web interface for listening for NSM API messages.</td>
<td>LAN</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>7800</td>
<td>Connections from managed devices to NSMXpress</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>7801</td>
<td>Connections from the NSM GUI Client to NSM</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>7802</td>
<td>Heartbeat between peers in an HA cluster</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>7803</td>
<td>Connections from managed IDP devices to NSM</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>7804</td>
<td>Connections from JUNOS devices, Secure Access devices, or Infranet Controller devices</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Out</td>
<td>22</td>
<td>SSH connection to new managed device</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>23</td>
<td>Telnet connection to new managed device</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>53</td>
<td>DNS lookups</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>80</td>
<td>System Security Updates from Juniper Networks</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>111</td>
<td>Shared Disk portmap lookup</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>123</td>
<td>Network Time Protocol (NTP) time synchronization</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>2049</td>
<td>Shared Disk NFS connection</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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

**Installing the Hardware**

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

To install NSMXpress:
1. Place the shipping container on a flat surface and remove the hardware components with care.

2. Remove the NSMxpress device from the shipping container and place it on a flat surface.

3. Mount NSMxpress in your server rack using the attached mounting brackets.

4. Plug the power cord into the AC receptacle on the rear panel.

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

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

   If your NSMxpress contains two power supplies, plug each power cord into a separate power circuit to ensure that the NSMxpress continues to receive power if one of the power circuits fails.

6. Plug the Ethernet cable into the port marked ETH0 on the front panel. See Figure 1 on page 6.

   Figure 1: Front Panel of NSMxpress

7. Plug the null modem serial cable into the console port. See Figure 1 on page 6.

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

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

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

   The internal port uses two LEDs to indicate the LAN connection status, which is described in Table 6 on page 7.

Hardware installation is now complete. The next step is to set up the software, as described in “Initial Setup Configuration” on page 7.

Table 6 on page 7 provides LED information for the ETH0 and ETH1 ports.
Table 6: Ethernet Port LEDs

<table>
<thead>
<tr>
<th>LAN Status</th>
<th>LED 1</th>
<th>LED2</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Mbps connection</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>100 Mbps connection</td>
<td>Green</td>
<td>Off</td>
</tr>
<tr>
<td>1000 Mbps connection</td>
<td>Orange</td>
<td>Off</td>
</tr>
<tr>
<td>Data is being transferred</td>
<td>Orange, Green, or Off</td>
<td>Blinking</td>
</tr>
<tr>
<td>No connection</td>
<td>Off</td>
<td>Off</td>
</tr>
</tbody>
</table>

Initial Setup Configuration

When you first turn on an unconfigured NSMXpress appliance, you need to enter basic network and machine information through the serial console to make your appliance accessible to the network. After entering these settings, you can continue configuring the appliance using the CLI or the Web interface. You are not prompted for the initial setup information again.

This section describes the required serial console setup and the tasks you need to perform when connecting to your NSMXpress for the first time:

- Boot NSMXpress on page 7
- Set Up Your Appliance on page 8

Boot NSMXpress

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

**Set Up Your Appliance**

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

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

1. Enter the IP address for interface eth0 and press Enter.
2. Enter the subnet mask for interface eth0 and press Enter.
3. Enter the default route or default gateway address for interface eth0 and press Enter.

Applying changes...
Re-loading database
ip_tables: (C) 2000–2002 Netfilter core team
ip_tables: (C) 2000–2002 Netfilter core team
ip_tables: (C) 2000–2002 Netfilter core team
Done!

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

To configure your system via command line, type:
nsm_setup

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

[admin@NSMXpress ~]$ ...

To complete the setup process using the CLI, go to “CLI Configuration” on page 8.
To complete the setup process using the Web interface, go to “Web Interface Configuration” on page 9.

**CLI Configuration**

To finish initial setup from the CLI, use the following steps. If you are logged in, enter nsm_setup at the command prompt.
If you are not logged on, follow these steps:

1. Enter your admin username, and then press Enter:

   Juniper NSMXpress OS build 2.105498
   NSM 2008.2r1
   Kernel 2.6.9-55.0.2.ELsmp on an i686

   NSMXpress.Juniper.net login: admin
   Password:
   Last login: Tue May 27 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 “Installing and Configuring NSM from the CLI” on page 11 for information about how to install and configure NSM on your NSMXpress appliance from the CLI.

*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.

*Web Interface Configuration*

To finish initial setup from a Web interface, use the following steps.
1. Copy the URL (starting with https://) from the terminal emulator after installing NSM Xpress:

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

2. Open a Web browser and paste the URL into the address text box.
3. Press Enter to open the NSM Xpress login page.
4. Enter the admin user name and password and then click Login.
5. See “Configuring NSM from the Web Interface” on page 31 for details about how to install and configure NSM on your NSM Xpress appliance from the Web interface.
Chapter 2

Installing and Configuring NSM from the CLI

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

- Navigating the Menus on page 11
- Configuring the NSM Software on page 13
- Configuring a Regional Server on page 14
- Configuring the Central Manager on page 19
- Configuring Standard Configuration Options on page 24
- NSMXpress Default Restoration on page 28

Navigating the Menus

As you configure NSM on your NSMXpress appliance, 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 options include:

- General Options on page 11
- Using nsm_setup on page 12

General Options

The NSM Configuration Main Menu has the following options:

NSM Configuration Main Menu

1> Management IP [10.150.43.205]
   The IP address on this server that will be used for management

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

3> GUI server one-time password []
   Password to initiate authentication between HA peers and to Central Manager. This password must be the same for all NSM servers in this installation.
4> NSM License type []
 Specify a license file, or select “Base Install”
to use the built-in limited device license.

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

Choice [1-4,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 take 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. This
option is last on most menus.

■ Quit—Enter Q to exit from the setup program. You will be prompted to save or
cancel any changes you made since you last saved:

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. Follow these steps to return to the NSMXpress setup program. The steps
in this procedure assume NSMXpress is connected to the computer running a terminal
emulation program. If not, see “Initial Setup Configuration” on page 7 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 NSM\textxpress and wait for the login prompt:

\begin{verbatim}
Juniper NSM\textxpress NSM 2008.2r1
Kernel 2.6.9-42.0.8.ELsmp on an i686
NSM\textxpress.juniper.net logon: admin
Password:
Login: Tue May 17 09:43:50 on tty50
Run NSM\textxpress 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@NSM\textxpress ~]$ 
\end{verbatim}

2. Log in using your “admin” user name and password.
3. Enter \texttt{nsm\_setup} at the prompt.
4. Enter your password and press Enter.
5. From the NSM\textxpress Settings menu:
   - For a regional server, enter \texttt{9}, and then enter \texttt{1} to display the NSM
     Configuration Main Menu for typical settings, or enter \texttt{2} for custom settings.
   - For a central manager, enter \texttt{9} to display the Configuration Main Menu.

\section*{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 section
describes that setup process.

The steps in this procedure assume you:
   - Have completed all appropriate steps in “Getting Started” on page 3.
   - Have a console terminal or terminal emulation utility running.
   - See the following command output in the emulation utility window:

\begin{verbatim}
Your NSM\textxpress is now active on the network.
To configure your system via a web browser, connect to:
  https://10.150.43.205/admin
To configure your system via command line, type:
nsm\_setup
For operation of NSM server, switch to user “nsm”
Please consult NSM product documentation for details.
[admin@NSM\textxpress ~]$
\end{verbatim}
Your NSMXpress appliance comes preconfigured as a regional server or a central manager, as described in the following sections:

- Configuring a Regional Server on page 14
- Configuring the Central Manager on page 19

## Configuring a Regional Server

For details on using the general setup menu items, see “Navigating the Menus” on page 11.

To configure the regional server, select one of the following options by number:

- **Typical Settings**—Enter 1 to select typical settings. This option provides a simplified menu to install a 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.

The following sections provide details of these options:

- Configuring Typical Settings on page 14
- Configuring Custom Settings on page 15

## Configuring Typical Settings

This section describes the options that are available for a typical installation for the regional server:

**NSM Configuration Main Menu**

1> **Management IP [10.150.43.205]**
   The IP address on this server that will be used for management

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

3> **GUI server one-time password []**
   Password to initiate authentication between HA peers and to Central Manager. This password must be the same for all NSM servers in this installation.

4> **NSM License type []**
   Specify a license file, or select “Base Install” to use the built-in limited device license.

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

Choice [1-4,A,C,R]:
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 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 privilege in NSM.

- **GUI Server one-time password**—Enter 3 to specify this password. This password authenticates this server to its peers in a high-availability configuration, and to the central manager.

- **NSM License type [Base Install]**—Enter 4 to specify 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 filename of the license file you purchased from Juniper Networks that permits you to manage more than 25 devices.

For additional details about NSM licensing, see the *Network and Security Manager Installation Guide*.

### Configuring 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 following two options:

5> **Menu: High Availability [Off]**

6> **Menu: Advanced Options**

You have the following options:

- **High Availability**—Enter 5 to open a menu to configure HA.

- **Advanced Options**—Enter 6 to open a menu of additional configurable options, including the port number for receiving messages through the NSM API, remote database replication details, and the Statistical Report Server (SRS).

The following sections provide details about these options:

- Configuring High Availability on page 16
- Configuring Advanced Options on page 17
Configuring High Availability

**NOTE:** When installing NSM regional server in a high availability configuration with a shared disk, you must first revert the system to factory default values using the boot menu. See “NSMXpress Default Restoration” on page 28 for details.

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 NSMXpress as either the primary or secondary server. At the next prompt, enter y for the primary server. Enter n for a 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 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. NSMXpress supports shared disks 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 *Network and Security Manager Installation Guide*.

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. 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 “Setting Interface Options” on page 25 for more information). Setting a redundant link is optional. For more information on options available to you for 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 the HA link count is set to 1, the only options available are to set the HA link count and to return to the High Availability menu. If the HA link count is set to 2, all options are available.

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. For more information on options available to you for custom settings, refer to the Network and Security Manager Installation Guide.

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

Configuring Advanced Options

The Advanced Options menu provides the following configuration options:

Menu: Advanced Options

1> https port for NBI service [8443]
   The port number to listen for NBI
   (Default is 8443)

2> Menu: Remote Replication of Database [Off]

3> Menu: SRS [Off]

M> Main Menu
R> Redraw menu

Choice [1-3,M,R]:

Configuring a Regional Server
You have the following options:

- **https port for NBI service**—Enter 1 to change the port number for listening for messages for the NSM API. In response to the prompt, enter a value in the range 1024 through 65535. Any number outside this range returns an error message. The default value is 8443.

- **Menu: Remote Replication of Database**—Enter 2 to display a menu of options for configuring the time of day to take the backup, the location of the backup, and timeout value.

- **Menu: SRS**—Enter 3 to open a menu to configure Statistical Report Server (SRS).

The following sections provide details about configuring remote backup and SRS:

- Enabling and Configuring Remote Replication of the Database on page 18
- Enabling and Configuring Statistical Report Server on page 19

### Enabling and Configuring Remote Replication of the Database

On the Advanced Options menu, enter 2 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:

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)

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

- Remote Replication of Database—Enter 1 to turn remote replication on or off. At the next prompt, enter y to change the state.

- 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 servers and you must establish an SSH trust relationship. See the *Network and Security Manager Installation Guide* for details.

- Remote Replication Timeout—Enter 4 to time out the remote backup. The valid range is 1-65535 seconds.
Enabling and Configuring Statistical Report Server

The following options are available to configure statistical report server (SRS):

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

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. At the next prompt, enter y to turn it on or 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. At least eight characters are required. The password is case sensitive.

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

Configuring the Central Manager

For details about using the general setup menu items, see “Navigating the Menus” on page 11.
This section describes the options that are available for a central manager configuration. The central manager main menu options are:

NSM Configuration Main Menu

1> Management IP [10.150.43.205]
The IP address on this server that will be used for management

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

3> GUI server one-time password []
Password for authentication between HA peers and to all Regional Servers

4> Menu: High Availability [Off]

5> Menu: Advanced Options

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

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

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 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.

- GUI Server one-time password—Enter 3 to specify this password. This password authenticates this server to its peer in a high-availability configuration, and to regional servers.

- Menu: High Availability—Enter 4 to open a menu to configure HA. See “Configuring High Availability” on page 21.

- Menu: Advanced Options—Enter 5 to open a menu of additional options, including the port number for receiving messages through the NSM API, and remote database replication details.

The following sections provide procedures for configuring HA and advanced options:

- Configuring High Availability on page 21
- Configuring Advanced Options on page 23
Configuring High Availability

To configure high availability (HA), from the NSM Configuration Main menu, enter 4. NSMxpress displays the High Availability menu:

1> High Availability [n]
   Whether to enable HA on this server or not

2> Primary Status [y]
   If 'y', this machine is a Primary Server
   and if 'n' this machine is a Secondary Server

3> HA Remote IP []
   IP address for the peer's primary
   heartbeat link

4> HA Link Failure Detection IP []
   IP address outside the HA cluster

5> HA Inter-server password []
   Shared password for heartbeat

6> Menu: Shared Disk [Off]

7> Menu: HA Links

8> Menu: HA Advanced Settings

The following options are available to configure 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. At the next prompt, enter y for a primary server; enter n for a 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 computer outside 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 help you configure a shared disk. NSMxpress supports shared disk via NFS only. Due to the data-intensive nature of NSM, we recommend gigabit speed links (1000 Mbps) for shared disk use. For more information on custom settings, refer to the Network and Security Manager Installation Guide.

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

2> Shared Disk Source (NFS) []
   Source of shared disk, e.g. /dev/sdc1
Menu: HA Links—Enter 7 to open the HA Links menu.

The options in this menu 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 (see “Setting Interface Options” on page 25 for details). Setting a redundant link is optional. For more information on options available to you for custom settings, refer to the *Network and Security Manager Installation Guide*.

If the HA link count is set to 1, the only options available are to set the HA link count and to return to the High Availability menu. If the HA link count is set to 2, all options are available.

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

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

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
**Configuring Advanced Options**

To configure advanced options, from the NSM Configuration Main menu, enter 5. NSMxpress displays the Advanced Options menu:

Menu: Advanced Options

1> https port for NBI service [8443]
   The port number to listen for NBI
   (Default is 8443)

2> Menu: Remote Replication of Database [Off]

M> Main Menu
R> Redraw menu

Choice [1-2,M,R]:

You have the following options:

- https port for NBI service—Enter 1 to change the port number for listening for messages for the NSM API. In response to the prompt, enter a value in the range 1025 through 65535. Any number outside this range returns an error message. The default value is 8443.

- Menu: Remote Replication of Database—Enter 2 to display a menu of options for configuring the time of day to take the backup, the location of the backup, and timeout value. See “Enabling and Configuring Remote Replication of the Database” on page 23.

**Enabling and Configuring Remote Replication of the Database**

On the Advanced Options menu, enter 2 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:

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 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)

The screen always shows the current status of the remote backup database. If no status exists, the option has not yet been configured.
Remote Replication of Database—Enter 1 to turn remote replication on or off. At the next prompt, enter y to change the state.

Hour of day to Replicate Database—Enter 2, and then specify the hour to start the backup. The valid range is 00-23.

Remote Backup IP—Enter 3 to specify 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.

Remote Replication Timeout—Enter 4 to change the timeout period for the remote backup. The valid range is 1-65535 seconds.

Configuring Standard Configuration Options

After the initial setup, continue configuring typical options, including the following tasks. 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.

Run nsm_setup to access these options on the NSMXpress Settings Menu:

- Changing the Password on page 24
- Setting Interface Options on page 25
- Setting Routing Options on page 25
- Changing the NSMXpress Hostname on page 26
- Adding DNS Servers on page 26
- Setting the System Time on page 26
- Forwarding Local Status E-mails on page 27
- Updating System Security on page 27
- Saving Setup Options on page 28

Changing the Password

To change your password:
1. On the NSMXpress Settings Menu, enter 1 at the prompt.
2. Enter y when prompted to change the password for an “admin” user.
3. Type 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 NSMXpress Settings menu.
**Setting Interface Options**

NSM Xpress has two ports labeled ETH0 and ETH1. During initial setup, you specify 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. On the NSM Xpress Settings menu, 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 NSM Xpress Settings 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 entering 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. Enter 1 for full duplex or 2 for half duplex, and then return to the NSM Xpress Settings menu.

**Setting Routing Options**

To set or modify routing options:

1. On the NSM Xpress Settings menu, enter 3 at the prompt.

2. Enter 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 NSM Xpress Settings menu.
2. To change the static routing options (optional).

Follow the prompts to add a new static route and return to the NSMxpress Settings menu.

**Changing the NSMxpress Hostname**

To change the hostname:

1. On the NSMxpress Settings menu, enter 4 at the prompt.
2. Enter y at the verification prompt to continue.
3. Enter the new hostname and press Enter to return to the NSMxpress Settings menu.

**NOTE:** If a hostname consisting of 4 or more labels is changed to a different hostname, also with 4 or more labels, the previous hostname alias might remain in the /etc/hosts file. This condition can be corrected by manually editing the /etc/hosts file.

**Adding 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. On the NSMxpress Settings menu, enter 5 at the prompt.
2. Enter 1 to add a nameserver.
3. When prompted, enter the new nameserver in dotted decimal notation.

**Setting the System Time**

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. On the NSMXpress Settings menu, enter 6 at the prompt.
2. Enter 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 NSMXpress Settings menu.
3. Enter 2 to set NTP servers.

   NTP servers automatically set the system clock based on external time sources.
4. Enter one of the following values at the prompt:
   - 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 NSMXpress Settings menu.

**Forwarding Local Status E-mails**

You can use this option to forward all local root e-mail messages 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. On the NSMXpress Settings menu, enter 7 at the prompt.
2. Enter 1 to add or change the recipient.
3. Enter 2 to remove the recipient.

**Updating System Security**

System security updates are NSMXpress operating system-level patches that protect the system against any future reported security vulnerabilities. NSMXpress checks for new updates daily by connecting to Juniper Networks.

To manage system security updates:
1. On the NSMXpress Settings menu, enter 8 at the prompt.
2. Enter one of the following values to select the option:
   - 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 NSMXpress version.
   - 4 to set the proxy for security update check.
3. Follow the prompts to manage security updates, and then return to the NSMxpress Settings menu.

**Saving Setup Options**

Before you configure the regional server or the central manager, NSMxpress opens the Apply Change submenu. If you quit out of a menu after making changes, NSMxpress also opens this screen and prompts you to save your changes. Updates are enabled by default.

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
B> 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:
- At the prompt, enter 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.
- Enter 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 reinstall NSMxpress, the appliance is completely reimaged. No user data remains on the system. If you want to preserve your database, back it up before reinstalling.

To reinstall NSMxpress, use the following procedure. The steps in the procedure assume NSMxpress is connected to the computer with a null-modem cable. If not, refer to the section “Initial Setup Configuration” on page 7 for details.

To reinstall 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:
Press any key to enter the menu

Booting NSMXPress
Booting NSMXpress
Booting NSMXpress
Booting NSMXpress
Booting NSMXpress
Booting NSMXpress
Booting NSMXpress

in 4 seconds...

3. Use the arrow keys to select **Re-Install current-version-number**, and then press Enter:

NSMXpress
Rescue
Re-Install <current-version-number>
Re-Install <previous-version-number>
Rescue Boot from Secondary Drive

4. Read the paragraph, and then press **Enter**.

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" as 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 task will take a few minutes.

When reinstallation is finished, you are prompted to reboot:

```
+-------------------------------------------------------------------|
| Congratulations, your Juniper NSMXpress Management Appliance 1.0  |
| 1386 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.
This chapter describes how to configure NSM from the NSMxpress Web interface. It contains the following sections:

- Configuring the NSM Software on page 31
- Managing NSM Administration on page 40
- Managing System Administration on page 45
- Maintaining NSMxpress on page 56
- Troubleshooting on page 58
- Viewing System Information on page 62

## Configuring the NSM Software

After logging in as an ‘admin’ user, an initial setup script walks you through additional configuration system settings before finalizing the NSM installation. This chapter describes that setup process.

Your NSMxpress appliance comes preconfigured as a regional server or a central manager. Most installation and configuration steps in this section are identical for both types of server. All exceptions are noted.

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

- Configuring Basic Settings on page 31
- Configuring High Availability on page 34
- Advanced Options on page 36
- Installing NSM Software on page 39

## Configuring Basic Settings

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

1. Complete all appropriate steps in “Getting Started” on page 3.
2. Enter the `https://<ip>/admin` URL for your appliance in a Web browser. See “Web Interface Configuration” on page 9 for details.
3. Log into the Web interface as an ‘admin’ user to open the Install NSM Regional Server window (see Figure 2 on page 32) or the Install NSM Central Manager window (see Figure 3 on page 33).

**NOTE:** The ‘admin’ user default username is admin and the password is the one you created in Step 6 of “Boot NSMXpress” on page 7.
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 after you click the second radio button.

5. 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.

6. 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.

7. 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.
8. Click **Submit** to save any changes, and then click **Install** to install the software.

### Configuring High Availability

To configure high availability (HA) settings:

1. On the NSM Configuration Main Menu, click **Menu** next to High Availability to access HA options. See Figure 4 on page 34.

#### Figure 4: High Availability Options

*Menu: High Availability*

- **High Availability**: Whether to enable HA on this server or not.
- **Primary Status**: If ‘y’, this machine is a Primary Server and if ‘n’ this machine is a Secondary Server.
- **HA Remote IP**: IP address for the peer’s primary heartbeat link.
- **HA Link Failure Detection IP**: IP address outside the HA cluster.
- **HA Inter-server password**: Shared password for heartbeat.
- **Shared Disk**: Off (Menu), HA Links (Menu), HA Advanced Settings (Menu)

2. Use the High Availability option to turn HA on (**y**) or off (**n**). The default is off.
3. Use the Primary Status option to set your NSMXpress appliance as either the primary or secondary server in the HA cluster. If you select **y**, it is the primary server (the default). If you select **n**, it is the secondary server.
4. Use the HA Remote IP option to enter the IP address for the HA peer in the HA cluster.
5. Use the HA Link Failure Detection IP option to enter the IP address of a computer outside the HA cluster that you can ping to verify connection status.
6. Use the HA Inter-server password option to enter the heartbeat password used between the primary and secondary servers.
7. Click **Submit** to save the changes.
8. Click **Menu** next to Shared Disk (see Figure 4 on page 34) to configure a shared disk for regional servers (see Figure 5 on page 35) or for central managers (see Figure 6 on page 35). This step is optional.
NSMXpress supports shared disk via NFS only. Due to the data-intensive nature of NSM, we recommend gigabit speed links (1000 Mbps) for shared disk use. For more information about custom settings, refer to the Network and Security Manager Installation Guide.

9. Click **Menu** next to HA Links (see Figure 4 on page 34) to configure the second link in the HA cluster (see Figure 7 on page 35). This step is optional.

**Figure 7: HA Links Options**

Use the options in this menu to set up a redundant link for the HA cluster. If you are going to use a second link, you need to set the IP address for eth1 before configuring this setting (see “Configuring the Network” on page 46 for details). Setting a redundant link is optional. For more information about custom settings, refer to the Network and Security Manager Installation Guide.
If you configure HA with just one heartbeat link, then device management traffic and data replication traffic both use that link. If you configure two links, device management traffic uses the first link and data replication uses the second.

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

**Figure 8: Redundant Links**

<table>
<thead>
<tr>
<th>Menu: HA Links</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HA Link count</td>
<td>2</td>
</tr>
<tr>
<td>Number of heartbeat links between the Primary and Secondary Servers</td>
<td></td>
</tr>
<tr>
<td>HA Link 2 Local IP</td>
<td></td>
</tr>
<tr>
<td>IP address for this machine's secondary heartbeat link</td>
<td></td>
</tr>
<tr>
<td>HA Link 2 Remote IP</td>
<td></td>
</tr>
<tr>
<td>IP address for the peer's secondary heartbeat link</td>
<td></td>
</tr>
<tr>
<td>HA Remote Replication IP</td>
<td></td>
</tr>
<tr>
<td>IP address used for remote HA replications</td>
<td></td>
</tr>
</tbody>
</table>

10. Click **Menu** next to HA Advanced Settings (see Figure 4 on page 34) to configure HA advanced settings (see Figure 9 on page 36). This step is optional.

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

**Figure 9: HA Advanced Settings**

<table>
<thead>
<tr>
<th>Menu: HA Advanced Settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HA Heartbeat Frequency</td>
<td>15</td>
</tr>
<tr>
<td>Time interval in seconds between heartbeat messages (Default is 15 seconds) (Range is 5 to 3600)</td>
<td></td>
</tr>
<tr>
<td>HA Heartbeat Failure Threshold</td>
<td>4</td>
</tr>
<tr>
<td>Number of missing heartbeat messages before automatic switchover occurs (Default is 4 missing messages) (Range is 1 to 10000)</td>
<td></td>
</tr>
<tr>
<td>HA Data Replication Timeout</td>
<td>1800</td>
</tr>
<tr>
<td>Psync Command Replication Timeout (Default is 1800 seconds) (Range is 1 to 85535)</td>
<td></td>
</tr>
</tbody>
</table>

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

**Advanced Options**

To display the Advanced Options menu, on the NSM Configuration Main Menu, select **Menu** next to Advanced Options. The Advanced Options menu appears as shown in Figure 10 on page 37.
Advanced installation options include:

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

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

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

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

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

- Enabling and Configuring Remote Replication of the Database on page 37
- Enabling and Configuring SRS (Regional Server Only) on page 38

**Enabling and Configuring Remote Replication of the Database**

To configure remote replication of database settings:
1. On the Advanced Options menu, click **Menu** next to Remote Replication of Database (see Figure 4 on page 34) to configure daily backups (see Figure 11 on page 38).

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Replication of Database</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hour of day to Replicate Database</td>
<td>02</td>
<td></td>
</tr>
<tr>
<td>Remote Backup IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Replication Timeout (seconds)</td>
<td>1800</td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

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

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

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

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

This option is not available on central manager. To configure statistical report server (SRS) settings:
1. On the Advanced Options menu, click **Menu** next to SRS (see Figure 4 on page 34) to open the SRS menu (see Figure 12 on page 39).

**Figure 12: SRS Menu**

![SRS Menu](image)

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

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

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

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

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

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

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

**Installing NSM Software**

After you submit all your configuration options, click **Install** to install the NSM software on your NSMXpress 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 40
- Downloading NSM MIBS (Regional Server Only) on page 40
- Exporting Audit Logs on page 41
- Exporting Device Logs (Regional Server Only) on page 41
- Generating Reports (Regional Server Only) on page 42
- Modifying NSM Configuration Files on page 42
- Backing Up the NSM Database on page 43
- Changing the NSM Management IP on page 44
- Scheduling Security Updates on page 44

Changing the Superuser Password

To change the superuser password, select NSM Administration > NSM Super User Password. See Figure 13 on page 40.

Figure 13: Change Superuser Password

![Change Password for Super User](image)

Downloading NSM MIBS (Regional Server Only)

To download any available MIBs, select NSM Administration > Download NSM MIBS, and then click Download MIB. See Figure 14 on page 41. This option is not available on central manager.
Exporting Audit Logs

To export audit logs, select NSM Administration > Export Audit Logs. See Figure 15 on page 41.

Exporting Device Logs (Regional Server Only)

To export device logs, select NSM Administration > Export Device Logs. See Figure 16 on page 41). This option is not available on central manager.
Generating Reports (Regional Server Only)

To generate reports, select NSM Administration > Generate Reports. See Figure 17 on page 42. This option is not available on central manager.

**Figure 17: Generate Reports**

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

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

Modifying NSM Configuration Files

To manually edit the GuiSrv.cfg, DevSrv.cfg, and HaSrv.cfg files, select NSM Administration > Modify NSM Configuration Files. The example in Figure 18 on page 43, shows the option to modify the GuiSrv.cfg file.
Figure 18: NSM Configuration Files

NSM Configuration Files

GuiSvc.cfg

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

The server will be restarted once the changes are made.

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

setuid.user = root
clientId = 0
serverGuiSvcId = 2
clientOneTimePassword = ds3008ns

default.printLevel = warn
default.printProperties = where=file,sync=0,maxfilenum=15
#statusMonitor.printLevel = debug
#statusMonitor.printProperties = where=file,sync=1,maxfilenum=250
#guiSvcDirectiveManager.printLevel = debug
#guiSvcDirectiveManager.printProperties = debug
#guiSvcLicenseManager.licenseFile = /usr/netscreen/GuiSvc/var/license/license.txt
#guiSvcLicenseManager.printLevel = debug
#guiSvcLicenseManager.printProperties = debug
```

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

Back up the NSM Database

To configure backups of the NSM database, select NSM Administration > NSM Database Backup link under NSM Administration. See Figure 19 on page 44.
Changing the NSM Management IP

To change the IP address of the NSM management server, select **NSM Administration > NSM Management IP** link under NSM Administration. See Figure 20 on page 44.

Scheduling Security Updates

To schedule security updates, select **NSM Administration > Schedule Security Updates**. See Figure 21 on page 45.
Figure 21: Schedule Security Updates

Managing System Administration

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

- Rebooting or Shutting Down NSMXpress on page 45
- Changing the User Password on page 46
- Configuring the Network on page 46
- Monitoring with SNMP on page 49
- Forwarding Syslog Messages on page 51
- Changing the System Time on page 55
- Installing Updates on page 56
- Configuring the Web Interface on page 56

Rebooting or Shutting Down NSMXpress

To reboot or shut down NSMXpress, select System Administration > Bootup and Shutdown, and then click either Reboot System or Shutdown System. See Figure 22 on page 45.

Figure 22: Boot Up and Shut Down
Changing the User Password

To change the user password, select System Administration > Change User Password, fill out the form shown in Figure 23 on page 46, and then click Change.

Figure 23: Change User Password

<table>
<thead>
<tr>
<th>Changing NSMXpress user password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Old password</td>
</tr>
<tr>
<td>New password</td>
</tr>
<tr>
<td>New password (again)</td>
</tr>
<tr>
<td>Clear form</td>
</tr>
</tbody>
</table>

Configuring the Network

To access options that allow you to configure the network, select System Administration > Network Configuration. The Network Configuration window appears as shown in Figure 24 on page 46.

Figure 24: Network Interfaces Options

Network Configuration

Click this button to activate the current boot-time interface and routing settings, as they normally would be after a reboot. Warning - this may make your system inaccessible via the network, and cut off access to NSMXpress.

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

- Network Interfaces on page 47
- Routing and Gateways on page 47
- Hostname and DNS Clients on page 48
- Host Addresses on page 48
**Network Interfaces**

Use this option to manage the network interfaces. See Figure 25 on page 47.

**Figure 25: Network Interfaces**

**Interfaces Active Now**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>IP Address</th>
<th>Netmask</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>Ethernet</td>
<td>172.24.66.111</td>
<td>255.255.252.0</td>
<td>Up</td>
</tr>
<tr>
<td>lo</td>
<td>Loopback</td>
<td>127.0.0.1</td>
<td>255.0.0.0</td>
<td>Up</td>
</tr>
</tbody>
</table>

**Interfaces Activated at Boot Time**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>IP Address</th>
<th>Netmask</th>
<th>Activate at boot?</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>Ethernet</td>
<td>172.24.66.111</td>
<td>255.255.252.0</td>
<td>Yes</td>
</tr>
<tr>
<td>eth1</td>
<td>Ethernet</td>
<td>From DHCP</td>
<td>Automatic</td>
<td>No</td>
</tr>
<tr>
<td>lo</td>
<td>Loopback</td>
<td>127.0.0.1</td>
<td>255.0.0.0</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Routing and Gateways**

Use this option to configure and manage routes and gateways. See Figure 26 on page 48.
Figure 26: Routes and Gateways

Routing configuration activated at boot time

Default routes

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

Act as router? □ Yes □ No

Static routes

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

Local routes

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

Save

Active Routes

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

Hostname and DNS Clients

Use this option to configure and manage hostnames and DNS clients. See Figure 27 on page 48.

Figure 27: DNS Client Options

DNS Client Options

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Resolution order</th>
<th>DNS servers</th>
<th>Search domains</th>
<th>Search domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSMXpress.juniper.net</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Update hostname in host addresses if changed?

Host Addresses

Use this option to manage host addresses. See Figure 28 on page 48.

Figure 28: Host Address

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

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

Delete Selected Host Addresses
**Monitoring with SNMP**

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

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

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

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

- SNMP Configuration on page 49
- SNMP System Information on page 50
- SNMP Trap Configuration on page 50

**SNMP Configuration**

To configure SNMP:

1. Select **System Administration > SNMP Monitoring**.
2. Select the **SNMP Config** tab, which is shown in Figure 29 on page 49.

**Figure 29: Configuring SNMP**

![SNMP Configuration Window]

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

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

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

6. Click **Save**.

**SNMP System Information**

To configure SNMP system information:

1. Select **System Administration** > **SNMP Monitoring**.
2. Select the **System Info** tab, which is shown in Figure 30 on page 50.

**Figure 30: Configuring SNMP System Information**

```
<table>
<thead>
<tr>
<th>Contact</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

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

4. Click **Save**.

**SNMP Trap Configuration**

To configure SNMP trap conditions:

1. Select **System Administration** > **SNMP Monitoring**.
2. Select the **SNMP Traps** tab, which is shown in Figure 31 on page 51.
3. In the Manager IP field, enter the IP address of the SNMP management server.

4. Select from the following trap conditions:
   - **Disk space low**
     Enter the percentage of free disk space below which SNMP issues a trap.
   - **Memory low**
     Enter the percentage of free memory below which SNMP issues a trap.
   - **CPU high**
     Enter the percentage of CPU use over which SNMP issues a trap.
   - **NSM start/stop**
   - **Admin Logon/Logoff**
   - **External IP unreachable**
     Enter the IP address of the required device.

5. Click **Save**.

**Forwarding Syslog Messages**

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

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

- Viewing Syslog Receivers on page 52
- Adding and Configuring Syslog Receivers on page 53
- Editing Syslog Receiver Configurations on page 55
- Deleting Syslog Receivers on page 55

**Viewing Syslog Receivers**

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

1. Select **System Administration > Syslog Forwarding**. The Syslog Forwarding window appears. Figure 32 on page 54 shows an example.

   **Syslog Forwarding**

   ![](image)

   **Table 7: Viewing Syslog Receivers**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver</td>
<td>A name provided by the network administrator to identify the syslog receiver</td>
</tr>
</tbody>
</table>

2. View the configured syslog receivers in the table in the top portion of the window. Table 7 on page 52 describes the fields.
### Table 7: Viewing Syslog Receivers (continued)

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

### Adding and Configuring Syslog Receivers

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

1. Select **System Administration > Syslog Forwarding**.
2. In the Data Sources section, select the syslog facility for each GUI Server log, Device Server log, and HA Server log. The syslog facility is a field included in the syslog message to help identify the data source.
3. Click **Save**.
4. Click **Add new Receiver**.

The syslog receiver configuration window appears as shown in Figure 32 on page 54.
5. In the Name field, enter a name for the syslog receiver. This is the name that the syslog receiver will be known by within NSM.

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

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

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

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

8. Click Save to save and apply the configuration.

**Editing Syslog Receiver Configurations**

To edit a syslog receiver configuration, follow these steps:

1. Select System Administration > Syslog Forwarding.

2. In the Syslog Receivers window, click the name of the syslog receiver you want to edit.

   The syslog receiver configuration window appears for the selected receiver.

3. Make the desired changes to the configuration.

4. Click Save to save and apply your edits to the configuration of this syslog receiver.

**Deleting Syslog Receivers**

To delete a syslog receiver configuration, follow these steps:

1. Select System Administration > Syslog Forwarding.

2. In the Syslog Receivers window, check the box next to each syslog receiver you want to delete.

3. Click Delete selected receivers.

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

**Changing the System Time**

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

■ Set or change the system time.

■ Set the time zone.

■ Configure an NTP server to synchronize the system time with an external clock.
Installing Updates

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

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

Configuring the Web Interface

To specify which NSM client computers can access NSMXpress through the Web interface, select System Administration > WebUI Configuration. The Allowed IP Addresses window appears as shown in Figure 33 on page 56.

Figure 33: Web Interface Access

Maintaining NSMXpress

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

- Viewing System Statistics on page 56

Viewing System Statistics

To view system statistics, select System Administration > Maintenance > System Statistics. The system Statistics window appears as shown in Figure 34 on page 57.
Figure 34: System Statistics

System Statistics

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

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

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

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

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

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

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

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

Troubleshooting

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

- Error Logs on page 58
- Network Utilities on page 59
- Tech Support on page 61

Error Logs

To review error logs, select **Troubleshooting > Error Logs**. Figure 35 on page 58 shows an example.

**Figure 35: Review Error Logs**

<table>
<thead>
<tr>
<th>Log File</th>
<th>Description</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>File: /usr/netscreen/DevSvr/var/errorLog/deviceDm.log</td>
<td>Device Server Error Log</td>
<td>View</td>
</tr>
<tr>
<td>File: /usr/netscreen/DevSvr/var/errorLog/prodDm.log</td>
<td>Data Collector Error Log</td>
<td>View</td>
</tr>
<tr>
<td>File: /usr/netscreen/DevSvr/var/errorLog/newLogWalker0.log</td>
<td>Log Walker Error Log</td>
<td>View</td>
</tr>
<tr>
<td>File: /usr/netscreen/DevSvr/var/errorLog/profileMgr0.log</td>
<td>Profiler Manager Error Log</td>
<td>View</td>
</tr>
<tr>
<td>File: /usr/netscreen/DevSvr/var/errorLog/statusMonitor0.log</td>
<td>Status Monitor</td>
<td>View</td>
</tr>
<tr>
<td>File: /usr/netscreen/GuiSvr/var/errorLog/guiDm.log</td>
<td>Gui Server Error Log</td>
<td>View</td>
</tr>
<tr>
<td>File: /usr/netscreen/GuiSvr/var/errorLog/guiMC.mc.log</td>
<td>Master Controller Error Log</td>
<td>View</td>
</tr>
<tr>
<td>File: /usr/netscreen/GuiSvr/var/errorLog/statusMonitor0.log</td>
<td>GuiSvc Status Monitor Error Log</td>
<td>View</td>
</tr>
<tr>
<td>File: /usr/netscreen/HaSvr/var/errorLog/highAvail0.log</td>
<td>High Avail Error Log</td>
<td>View</td>
</tr>
</tbody>
</table>

To view details of an individual error log, select the file you want to view and click **View**. Figure 36 on page 58 shows sample error log details.

**Figure 36: Error Log Detail**

View Logfile

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

Last 20 lines of Only show lines with text

```
est: /usr/netscreen/DevSvr/var/errorLog/gproDMM.log: No such file or directory
```

Last 20 lines of Only show lines with text

Refresh
Network Utilities

To access basic network utilities (ping, traceroute, and nslookup) for TCP/IP Networking, select Troubleshooting > Network Utilities. These tools also provide an IP subnet calculator. See Figure 37 on page 59.

**Figure 37: Network Utilities Options**

| Ping | Traceroute | Lookup | IP Subnet Calculator |

**Ping**

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

Figure 38 on page 59 shows an example.

**Figure 38: Ping Utility**

How Many Packets
Packet Size
Pattern(s) to send (Hex)?
How Many Sec Between Sending Each Packet?
Pattern(s) to send (Hex)?

**How Many Packets**

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

**Packet Size**

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

**How Many Sec Between Sending Each Packet**

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

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

**Verbosity Output**

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

**Numeric Output Only**

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

**Bypass Routing Tables**

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

**Traceroute**

Traceroute is a tool to print the route a packet takes to a network host. See Figure 39 on page 60.

**Figure 39: Traceroute Utility**

```plaintext
Module Index
Help...

Hostname: _____________________________

☐ Verbosity Output?
☐ Numeric Output only?
☐ Bypass routing tables?
☐ Use ICMP instead of UDP?
☐ Toggle Checksums?
☐ Socket level debugging?

How many Hops? ____________________ 30
Packet Length? _____________________ 40
How many sec between sending each packet? 5
Initial time-to-live? ________________ 1
Interface: __________________________

Trace It!
```

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

Use the lookup tool to obtain the IP address from a hostname and the hostname from an IP address (see Figure 40 on page 61). The query type drop-down list contains several types of records found in the DNS database. Enter a nameserver or select the default. If you choose the default, nslookup will use the server on which NSMXpress is installed.

Figure 40: Lookup Utility

IP Subnet Calculator

Use the IP subnet calculator to calculate the netmask for a TCP/IP-network. You can calculate a netmask by class and subnet bits or by the number of hosts (see Figure 41 on page 61). When you calculate a netmask by the number of hosts, NSMXpress returns the smallest network available.

Figure 41: IP Subnet Calculator

Tech Support

To get contact information for Juniper Networks technical support, select Troubleshooting > Tech Support under Troubleshooting. To help analyze problems, select a detail type in the drop-down list box, and then click Run Tech-Support Script. NSMXpress creates a file you can download and send to Juniper Networks technical support. See Figure 42 on page 62.
Figure 42: Juniper Tech Support

**Tech Support**

- Details from GUI, Device and HA servers

**Run Tech-Support Script**

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

**JTAC PHONE NUMBER:** 1-800-314-JTAC

**JTAC FTP SITE:** ftp.juniper.net

## Viewing System Information

Use the System Information menu item to display information about the server, including CPU load and memory use, as shown in Figure 43 on page 62.

Figure 43: System Information
Part 2
Appendixes

- NSMXpress LEDs on page 65
Appendix A

NSMXpress LEDs

This appendix describes the LEDs on the NSMXpress appliance.

- NSMXpress LEDs on page 65

NSMXpress LEDs

The front panel of the NSMXpress appliance has the following LEDs:

- TEMP—temperature
- PS FAIL—power supply failure
- HDD—hard drive
- PWR—power

Table 8 on page 65 describes their states.

Table 8: NSMXpress LEDs

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>TEMP</td>
<td>Unlit</td>
<td>The temperature is within normal the operating range.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Blinking red</td>
<td>A fan has failed, but the temperature is still within tolerance and the appliance continues to operate.</td>
<td>Replace the fan.</td>
</tr>
<tr>
<td></td>
<td>Solid red</td>
<td>The temperature has exceeded 120°C. The appliance powers down.</td>
<td>Replace the fan.</td>
</tr>
<tr>
<td>PS FAIL</td>
<td>Unlit</td>
<td>Power supplies are functioning normally.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Glows red and an audible alarm sounds</td>
<td>A power supply has failed.</td>
<td>Replace the power supply.</td>
</tr>
</tbody>
</table>
Table 8: NSMXpress LEDs (continued)

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDD</td>
<td>Unlit</td>
<td>No hard drive activity.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Blinking amber</td>
<td>Hard drive activity.</td>
<td></td>
</tr>
<tr>
<td>PWR</td>
<td>Unlit</td>
<td>The power is off.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>The power is on.</td>
<td></td>
</tr>
</tbody>
</table>
Part 3
Index

- Index on page 69
Index

A

admin user.................................................................9
Advanced Options menu
   central manager..................................................23, 36
   regional server...................................................17, 36
Apply Change menu.....................................................28
audit logs, exporting..................................................41

B

backup..............................................................................43

C

central manager
   configuring with CLI..............................................19
   configuring with Web interface...............................31
CLI, configuring NSMXpress from...............................8, 11
configuration files, editing............................................42
console port....................................................................6
console terminal, configuring...........................................7
CPU load........................................................................57
CPU use..........................................................................57
customer support..........................................................xviii
   contacting JTAC.......................................................xviii

D

database
   backing up.............................................................43
   remote replication of..............................................18, 23, 37
default gateway
   address.......................................................................8, 25, 47
default gateway, address..............................................8, 25, 47
defaults, restoring.......................................................28
device logs, exporting..................................................41
DevSvr cfg file...............................................................42
disk usage.......................................................................57
DMZ...............................................................................4
DNS client.......................................................................48
DNS server.....................................................................26
documentation set
   comments on...........................................................xviii

E
e-mail, forwarding......................................................27
e-error customer customers...........................................3
error logs.......................................................................58
eh0
   activity.......................................................................57
   configuring.............................................................25
   IP address...................................................................8
   LED............................................................................6
   subnet mask...........................................................8
eh1
   activity.......................................................................57
   configuring.............................................................25
   LED............................................................................6
   Ethernet cable............................................................6
   Ethernet port
      cabling.....................................................................6
      configuring.............................................................25
      LED........................................................................6
   external clock...........................................................27, 55

G

GUI Server one-time password.................................15, 20, 33
GuiSvr.cfg file...............................................................42

H

HA Advanced Settings menu..................................17, 22, 36
HA Links menu.........................................................16, 22, 35
hardware components.......................................................5
hardware installation.......................................................5
HaSvr.cfg file.................................................................42
heartbeat, configuring.................................................16, 22, 35
high availability
   central manager, configuring...................................21, 34
   regional server, configuring.....................................16, 34
High Availability menu
   central manager.......................................................21
   regional server.......................................................16
host address...................................................................48
hostname.......................................................................26, 48
# Index

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install NSM Central Manager window</td>
<td>32</td>
</tr>
<tr>
<td>Install NSM Regional Server window</td>
<td>32</td>
</tr>
<tr>
<td>interfaces, configuring</td>
<td>25, 47</td>
</tr>
<tr>
<td>IP address, configuring</td>
<td>8</td>
</tr>
<tr>
<td>IP subnet calculator</td>
<td>61</td>
</tr>
<tr>
<td>LEDs</td>
<td>6</td>
</tr>
<tr>
<td>license, NSM</td>
<td>15, 33</td>
</tr>
<tr>
<td>log rate</td>
<td>57</td>
</tr>
<tr>
<td>lookup utility</td>
<td>61</td>
</tr>
<tr>
<td>management IP</td>
<td>6</td>
</tr>
<tr>
<td>central manager</td>
<td>20, 33</td>
</tr>
<tr>
<td>changing</td>
<td>44</td>
</tr>
<tr>
<td>regional server</td>
<td>15, 33</td>
</tr>
<tr>
<td>manuals</td>
<td>xviii</td>
</tr>
<tr>
<td>comments on</td>
<td></td>
</tr>
<tr>
<td>memory usage</td>
<td>57</td>
</tr>
<tr>
<td>MIBs</td>
<td>40</td>
</tr>
<tr>
<td>mounting brackets</td>
<td>6</td>
</tr>
<tr>
<td>NBI See NSM API</td>
<td></td>
</tr>
<tr>
<td>network activity</td>
<td>57</td>
</tr>
<tr>
<td>network utilities</td>
<td></td>
</tr>
<tr>
<td>IP subnet calculator</td>
<td>61</td>
</tr>
<tr>
<td>lookup</td>
<td>61</td>
</tr>
<tr>
<td>ping</td>
<td>59</td>
</tr>
<tr>
<td>traceroute</td>
<td>60</td>
</tr>
<tr>
<td>network, configuring</td>
<td>46</td>
</tr>
<tr>
<td>northbound interface See NSM API</td>
<td></td>
</tr>
<tr>
<td>NSM</td>
<td></td>
</tr>
<tr>
<td>configuration files, editing</td>
<td>42</td>
</tr>
<tr>
<td>installing</td>
<td>39</td>
</tr>
<tr>
<td>updating</td>
<td>56</td>
</tr>
<tr>
<td>NSM API</td>
<td></td>
</tr>
<tr>
<td>port for central manager</td>
<td>23</td>
</tr>
<tr>
<td>port for regional server</td>
<td>18, 37</td>
</tr>
<tr>
<td>NSM Configuration Main Menu</td>
<td></td>
</tr>
<tr>
<td>central manager</td>
<td>19</td>
</tr>
<tr>
<td>regional server</td>
<td>14</td>
</tr>
<tr>
<td>NSM license</td>
<td>15, 33</td>
</tr>
<tr>
<td>ns user</td>
<td>9</td>
</tr>
<tr>
<td>nsms_setup utility</td>
<td>12</td>
</tr>
<tr>
<td>NSMXpress Settings menu</td>
<td>24</td>
</tr>
<tr>
<td>NTP server</td>
<td>27, 55</td>
</tr>
<tr>
<td>null modem serial cable</td>
<td>6</td>
</tr>
<tr>
<td>password</td>
<td>24</td>
</tr>
<tr>
<td>admin user</td>
<td></td>
</tr>
<tr>
<td>GUI server, one-time</td>
<td>15, 20, 33</td>
</tr>
<tr>
<td>heartbeat</td>
<td>16, 21, 34</td>
</tr>
<tr>
<td>NSM, central manager</td>
<td>20</td>
</tr>
<tr>
<td>super user, central manager</td>
<td>33, 40</td>
</tr>
<tr>
<td>super user, regional server</td>
<td>15, 33, 40</td>
</tr>
<tr>
<td>process count</td>
<td>57</td>
</tr>
<tr>
<td>reboot</td>
<td>45</td>
</tr>
<tr>
<td>regional server</td>
<td></td>
</tr>
<tr>
<td>configuring with CLI</td>
<td>14</td>
</tr>
<tr>
<td>configuring with Web interface</td>
<td>31</td>
</tr>
<tr>
<td>custom settings</td>
<td>15</td>
</tr>
<tr>
<td>typical settings, configuring</td>
<td>14</td>
</tr>
<tr>
<td>reinstallation</td>
<td>28</td>
</tr>
<tr>
<td>Remote Replication of Database menu</td>
<td>18, 23, 37</td>
</tr>
<tr>
<td>reports</td>
<td>42</td>
</tr>
<tr>
<td>root user</td>
<td>9</td>
</tr>
<tr>
<td>routing</td>
<td></td>
</tr>
<tr>
<td>default gateway</td>
<td>25, 47</td>
</tr>
<tr>
<td>static</td>
<td>25, 47</td>
</tr>
<tr>
<td>secondary server, configuring</td>
<td>16, 21, 34</td>
</tr>
<tr>
<td>security, updating</td>
<td>27, 44</td>
</tr>
<tr>
<td>shutdown</td>
<td>16, 21, 34</td>
</tr>
<tr>
<td>SNMP</td>
<td>45</td>
</tr>
<tr>
<td>authentication</td>
<td>49</td>
</tr>
<tr>
<td>configuring</td>
<td>49</td>
</tr>
<tr>
<td>monitoring NSMXpress with</td>
<td>49</td>
</tr>
<tr>
<td>system information for</td>
<td>50</td>
</tr>
<tr>
<td>trap configuration</td>
<td>50</td>
</tr>
<tr>
<td>SRS See Statistical Report Server</td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td>5</td>
</tr>
<tr>
<td>static routing</td>
<td>25, 47</td>
</tr>
<tr>
<td>Statistical Report Server menu</td>
<td>19, 38</td>
</tr>
<tr>
<td>Statistical Report Server, configuring</td>
<td>19, 38</td>
</tr>
<tr>
<td>subnet calculator</td>
<td>61</td>
</tr>
<tr>
<td>subnet mask, configuring</td>
<td>8</td>
</tr>
<tr>
<td>sudo su - nsm</td>
<td>9</td>
</tr>
<tr>
<td>support, technical See technical support</td>
<td></td>
</tr>
<tr>
<td>syslog</td>
<td>51</td>
</tr>
<tr>
<td>forwarding</td>
<td></td>
</tr>
<tr>
<td>receivers, adding</td>
<td>53</td>
</tr>
<tr>
<td>receivers, configuring</td>
<td>53</td>
</tr>
</tbody>
</table>
receivers, deleting ................................................. 55
receivers, editing .................................................. 55
receivers, viewing ................................................. 52
system information ...................................................... 62
system logs .................................................................. 58
system statistics ........................................................... 56
system time ........................................................... 26, 55

t
technical support ......................................................... 61
  contacting JTAC ....................................................... xviii
tiling ............................................................................. 58
time zone ..................................................................... 27, 55
time, setting .................................................................... 26, 55
traceroute utility ........................................................... 60
trap conditions, SNMP .................................................. 50
troubleshooting ............................................................ 58

u
URL, Web interface ...................................................... 10
user
  admin, nsm, root ....................................................... 9

w
Web interface
  configuring .................................................................... 56
  login URL ..................................................................... 10
Web interface configuration
  configuration .................................................................... 9
Web login ..................................................................... 10

y
Yum server ................................................................. 56