



# Juniper Networks Network and Security Manager

NSMXpress and NSM3000 User Guide

Release

# 2010.2



Published: 2010-05-17

Revision 1

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

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986–1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

*NSMXpress and NSM3000 User Guide*  
Copyright © 2010, Juniper Networks, Inc.  
All rights reserved. Printed in USA.

Writing: James Thomas  
Editing: Laura Singer  
Cover Design: Edmonds Design

Revision History  
May 18, 2010—Revision 1

The information in this document is current as of the date listed in the revision history.

## 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 Customer 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 or delay with its responsibilities herein. 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 III) 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 présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, 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

	<b>About This Guide</b> .....	<b>xv</b>
	Objectives .....	xv
	Audience .....	xv
	Conventions .....	xv
	Documentation .....	xvii
	Documentation Feedback .....	xviii
	Requesting Technical Support .....	xviii
	Self-Help Online Tools and Resources .....	xix
	Opening a Case with JTAC .....	xix
<b>Part 1</b>	<b>Using the NSM Appliance</b>	
<b>Chapter 1</b>	<b>Getting Started</b> .....	<b>3</b>
	About the NSM Appliances .....	3
	Installation and Configuration Workflow .....	4
	Hardware Installation .....	4
	NSM Appliance Ports .....	4
	Installing the NSMXpress Hardware .....	5
	Installing the NSM3000 Hardware .....	7
	Initial Setup Configuration .....	8
	Boot the NSM Appliance .....	8
	Set Up Your Appliance .....	9
	CLI Configuration .....	10
	Web Interface Configuration .....	10
<b>Chapter 2</b>	<b>Installing and Configuring NSM from the CLI</b> .....	<b>13</b>
	Navigating the Menu .....	13
	General Options .....	13
	Using nsm_setup .....	14
	Configuring the NSM Software .....	15
	Configuring a Regional Server .....	16
	Configuring Typical Settings .....	16
	Configuring Custom Settings .....	17
	Configuring High Availability .....	17
	Configuring Advanced Options .....	19
	Configuring the Central Manager .....	21
	Configuring High Availability .....	22
	Configuring Advanced Options .....	24
	Enabling and Configuring Remote Replication of the Database .....	24

	Configuring Standard Configuration Options . . . . .	25
	Changing the Password . . . . .	25
	Setting Interface Options . . . . .	26
	Setting Routing Options . . . . .	27
	Changing the NSM Appliance Hostname . . . . .	27
	Adding DNS Servers . . . . .	27
	Setting the System Time . . . . .	27
	Forwarding Local Status E-mails . . . . .	28
	Updating System Security . . . . .	28
	Saving Setup Options . . . . .	29
	The NSM Appliance Default Restoration . . . . .	29
<b>Chapter 3</b>	<b>Configuring NSM from the Web Interface . . . . .</b>	<b>31</b>
	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 . . . . .	39
	Changing the Superuser Password . . . . .	39
	Downloading NSM MIBS (Regional Server Only) . . . . .	40
	Exporting Audit Logs . . . . .	40
	Exporting Device Logs (Regional Server Only) . . . . .	40
	Generating Reports (Regional Server Only) . . . . .	41
	Modifying NSM Configuration Files . . . . .	41
	Backing Up the NSM Database . . . . .	42
	Changing the NSM Management IP . . . . .	43
	Scheduling Security Updates . . . . .	43
	Managing System Administration . . . . .	44
	Rebooting or Shutting Down the NSM Appliance . . . . .	44
	Changing the User Password . . . . .	45
	Configuring the Network . . . . .	45
	Network Interfaces . . . . .	45
	Routing and Gateways . . . . .	46
	Hostname and DNS Clients . . . . .	46
	Host Addresses . . . . .	47
	Managing RADIUS Servers . . . . .	47
	Adding a RADIUS Server . . . . .	48
	Changing the Priority of RADIUS Servers . . . . .	49
	Deleting a RADIUS Server . . . . .	49
	Editing RADIUS Server Parameters . . . . .	49
	Monitoring with SNMP . . . . .	50
	SNMP Configuration . . . . .	50
	SNMP System Information . . . . .	51
	SNMP Trap Configuration . . . . .	52

	Forwarding Syslog Messages . . . . .	53
	Viewing Syslog Receivers . . . . .	53
	Adding and Configuring Syslog Receivers . . . . .	54
	Editing Syslog Receiver Configurations . . . . .	56
	Deleting Syslog Receivers . . . . .	56
	Changing the System Time . . . . .	56
	Installing Updates . . . . .	56
	Managing Users . . . . .	57
	Creating New NSM Appliance Users . . . . .	57
	Deleting a User . . . . .	58
	Editing User Attributes . . . . .	59
	Understanding User Profiles . . . . .	59
	Configuring the Web Interface . . . . .	60
	Maintaining NSM Appliances . . . . .	61
	Viewing System Statistics . . . . .	61
	CPU . . . . .	61
	Log Rate . . . . .	61
	CPU Load . . . . .	61
	Memory Data . . . . .	62
	Network Data . . . . .	62
	Process Count . . . . .	62
	Disk Data . . . . .	62
	Tile All Graphs . . . . .	62
	Upgrading the Recovery Partition . . . . .	62
	Troubleshooting . . . . .	63
	Auditing User Operations . . . . .	63
	Error Logs . . . . .	65
	Network Utilities . . . . .	66
	Ping . . . . .	66
	Traceroute . . . . .	67
	Lookup . . . . .	68
	IP Subnet Calculator . . . . .	68
	Tech Support . . . . .	68
	Viewing System Information . . . . .	69
<b>Part 2</b>	<b>Appendixes</b>	
<b>Appendix A</b>	<b>NSMXpress LEDs . . . . .</b>	<b>73</b>
	NSMXpress LEDs . . . . .	73
<b>Part 3</b>	<b>Index</b>	
	Index . . . . .	77



# List of Figures

<b>Part 1</b>	<b>Using the NSM Appliance</b>	
<b>Chapter 1</b>	<b>Getting Started</b> .....	<b>3</b>
	Figure 1: Front Panel of NSMXpress .....	6
	Figure 2: Rear Panel of NSM3000 .....	7
	Figure 3: Front Panel of NSM3000 .....	8
<b>Chapter 3</b>	<b>Configuring NSM from the Web Interface</b> .....	<b>31</b>
	Figure 4: Regional Server Configuration Main Menu .....	32
	Figure 5: Central Manager Configuration Main Menu .....	33
	Figure 6: High Availability Options .....	34
	Figure 7: Shared Disk Options for Regional Servers .....	35
	Figure 8: Shared Disk Options for Central Managers .....	35
	Figure 9: HA Links Options .....	35
	Figure 10: Redundant Links .....	36
	Figure 11: HA Advanced Settings .....	36
	Figure 12: Advanced Options Menu .....	36
	Figure 13: Remote Replication of Database Options .....	37
	Figure 14: SRS Menu .....	38
	Figure 15: Change Superuser Password .....	39
	Figure 16: Download NSM MIBs .....	40
	Figure 17: Export Audit Logs .....	40
	Figure 18: Export Device Logs .....	40
	Figure 19: Generate Reports .....	41
	Figure 20: NSM Configuration Files .....	42
	Figure 21: Database Backup .....	43
	Figure 22: Change Management IP .....	43
	Figure 23: Schedule Security Updates .....	44
	Figure 24: ReBoot or Shut Down .....	44
	Figure 25: Change User Password .....	45
	Figure 26: Network Interfaces Options .....	45
	Figure 27: Network Interfaces .....	46
	Figure 28: Routes and Gateways .....	46
	Figure 29: DNS Client Options .....	47
	Figure 30: Host Address .....	47
	Figure 31: RADIUS Servers Dialog Box .....	48
	Figure 32: Add RADIUS Server Dialog Box .....	48
	Figure 33: Edit RADIUS Server Dialog Box .....	50
	Figure 34: Configuring SNMP .....	51
	Figure 35: Configuring SNMP System Information .....	51
	Figure 36: Configuring SNMP Traps .....	52

Figure 37: Configuring a Syslog Receiver . . . . .	55
Figure 38: NSMXpress Users Dialog Box . . . . .	57
Figure 39: Create NSMXpress User Dialog Box . . . . .	58
Figure 40: NSMXpress Users Dialog Box . . . . .	58
Figure 41: Web Interface Access . . . . .	61
Figure 42: System Statistics . . . . .	61
Figure 43: NSMXpress Actions Dialog Box . . . . .	64
Figure 44: Search Results Dialog Box . . . . .	65
Figure 45: Review Error Logs . . . . .	65
Figure 46: Error Log Detail . . . . .	66
Figure 47: Network Utilities Options . . . . .	66
Figure 48: Ping Utility . . . . .	66
Figure 49: Traceroute Utility . . . . .	67
Figure 50: Lookup Utility . . . . .	68
Figure 51: IP Subnet Calculator . . . . .	68
Figure 52: Juniper Tech Support . . . . .	69
Figure 53: System Information . . . . .	69

# List of Tables

	<b>About This Guide</b> .....	<b>xv</b>
	Table 1: Notice Icons .....	xvi
	Table 2: Text Conventions .....	xvi
	Table 3: Syntax Conventions .....	xvii
	Table 4: Network and Security Manager Publications .....	xvii
<b>Part 1</b>	<b>Using the NSM Appliance</b>	
<b>Chapter 1</b>	<b>Getting Started</b> .....	<b>3</b>
	Table 5: Required Ports on an NSM Appliance .....	5
	Table 6: Ethernet Port LEDs .....	6
<b>Chapter 3</b>	<b>Configuring NSM from the Web Interface</b> .....	<b>31</b>
	Table 7: Viewing Syslog Receivers .....	54
	Table 8: NSM Appliance WebUI User Profiles and Permissions .....	59
<b>Part 2</b>	<b>Appendixes</b>	
<b>Appendix A</b>	<b>NSMExpress LEDs</b> .....	<b>73</b>
	Table 9: NSMExpress LEDs .....	73



# 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 and NSM3000 are appliance versions 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 and NSM3000 run NSM 2010.2.

NSM appliances simplify the complexity of device administration by providing single, integrated management interfaces that control device parameters. Each appliance is preconfigured as either a regional server or central manager.

This guide describes how you can install NSM onto your NSM appliances. In addition, this guide describes how to manage the appliance using the NSM 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 you see 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





Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

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

Table 2: Text Conventions

Convention	Description	Examples
<b>Bold typeface like this</b>	<ul style="list-style-type: none"> <li>Represents commands and keywords in text.</li> <li>Represents keywords</li> <li>Represents UI elements</li> </ul>	<ul style="list-style-type: none"> <li>Issue the <b>clock source</b> command.</li> <li>Specify the keyword <b>exp-msg</b>.</li> <li>Click <b>User Objects</b></li> </ul>
<b>Bold typeface like this</b>	Represents text that the user must type.	<b>user input</b>
fixed-width font	Represents information as displayed on the terminal screen.	<pre>host1# show ip ospf Routing Process OSPF 2 with Router ID 5.5.0.250 Router is an area Border Router (ABR)</pre>
Key names linked with a plus (+) sign	Indicates that you must press two or more keys simultaneously.	Ctrl + d
<i>Italics</i>	<ul style="list-style-type: none"> <li>Emphasizes words</li> <li>Identifies variables</li> </ul>	<ul style="list-style-type: none"> <li>The product supports two levels of access, <i>user</i> and <i>privileged</i>.</li> <li><i>clusterID</i>, <i>ipAddress</i>.</li> </ul>
The angle bracket (>)	Indicates navigation paths through the UI by clicking menu options and links.	<b>Object Manager &gt; User Objects &gt; Local Objects</b>

Table 3 on page xvii defines syntax conventions used in this guide.

**Table 3: Syntax Conventions**

Convention	Description	Examples
Words in plain text	Represent keywords	terminal length
Words in italics	Represent variables	<i>mask, accessListName</i>
Words separated by the pipe (   ) symbol	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.	diagnostic   line
Words enclosed in brackets ( [ ] )	Represent optional keywords or variables.	[ internal   external ]
Words enclosed in brackets followed by and asterisk ( [ ]*)	Represent optional keywords or variables that can be entered more than once.	[ level1   level2   11 ]*
Words enclosed in braces ( { } )	Represent required keywords or variables.	{ permit   deny } { in   out } { clusterId   ipAddress }

## Documentation

Table 4 on page xvii describes documentation for NSM.

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

Book	Description
<i>Network and Security Manager Installation Guide</i>	Describes the steps to install the NSM management system on a single server or on separate servers. It also includes information on how to install and run the NSM user interface. This guide is intended for IT administrators responsible for the installation or upgrade of NSM.
<i>Network and Security Manager Administration Guide</i>	Describes how to use and configure key management features in the NSM. It provides conceptual information, suggested workflows, and examples. This guide is best used in conjunction with the NSM Online Help, which provides step-by-step instructions for performing management tasks in the NSM user interface (UI).  This guide is intended for application administrators or those individuals responsible for owning the server and security infrastructure and configuring the product for multiuser systems. It is also intended for device configuration administrators, firewall and VPN administrators, and network security operation center administrators.
<i>Network and Security Manager Configuring ScreenOS Devices Guide</i>	Describes NSM features related to device configuration and management. It also explains how to configure basic and advanced NSM functionality, including deploying new device configurations, managing security policies and VPNs, and general device administration.

Table 4: Network and Security Manager Publications (*continued*)

Book	Description
<i>Network and Security Manager Online Help</i>	Provides procedures for basic tasks in the NSM user interface. It also includes a brief overview of the NSM system and a description of the GUI elements.
<i>Network and Security Manager API Guide</i>	Provides complete syntax and a description of the Simple Object Access Protocol (SOAP) messaging interface to NSM.
<i>Network and Security Manager Release Notes</i>	<p>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.</p> <p>Release Notes are included on the corresponding software CD and are available on the Juniper Networks Website.</p>
<i>NSMXpress and NSM3000 User Guide</i>	Describes how to set up and manage an NSM appliance as a central manager or regional server.

## 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](mailto: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/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

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

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

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

## Opening a Case with JTAC

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

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

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



## PART 1

# Using the NSM Appliance

Part 1 contains the following chapters:

- Getting Started on page 3
- Installing and Configuring NSM from the CLI on page 13
- Configuring NSM from the Web Interface on page 31



## CHAPTER 1

# Getting Started

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

This chapter contains the following sections:

- About the NSM Appliances on page 3
- Hardware Installation on page 4
- Initial Setup Configuration on page 8

## About the NSM Appliances

---

NSMXpress and NSM3000 are appliance versions of Network and Security Manager (NSM) and run NSM 2010.2. NSM appliances simplify the complexity of network administration by providing single, integrated management interfaces that control device parameters.

These robust hardware management systems install 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 appliances because it eliminates the need to have dedicated resources for maintaining a network and security management solution.

NSM appliances make it easy for administrators to control device configuration, network settings, and security policy settings for multiple families of Juniper Networks devices including:

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

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

Up to 10 administrators can log into an NSM appliance concurrently.

## Installation and Configuration Workflow

This guide explains the steps for installing and configuring an NSM appliance and for configuring NSM.

1. Install the NSM appliance hardware.
2. Set up the NSM appliance using the serial port.
3. Configure the NSM appliance software using either the CLI or the Web interface.
4. Configure the NSM software which is preinstalled in the NSM appliance, with site-specific parameters.

## Hardware Installation

---

We recommend that you install the NSM appliance 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 an NSM appliance in your DMZ, ensure that it can connect to your internal resources.

## NSM Appliance Ports

Table 5 on page 5 provides required port information on the NSM appliances.

Table 5: Required Ports on an NSM Appliance

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

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

## Installing the NSMXpress 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.

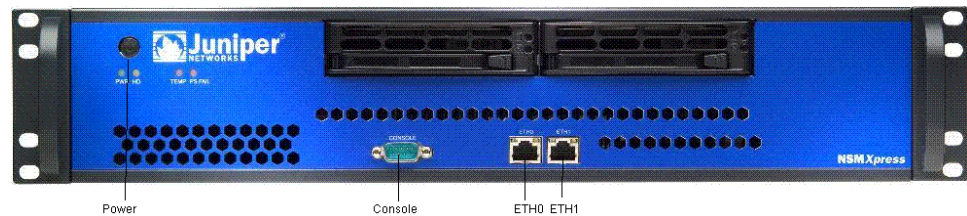
If your NSMXpress contains two power supplies, plug a power cord into each AC receptacle.

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 3 on page 8.

Figure 1: Front Panel of NSMXpress



7. Plug the null modem serial cable into the console port. See Figure 3 on page 8.

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 6.

Hardware installation is now complete. The next step is to set up the software, as described in "Initial Setup Configuration" on page 8.

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

Table 6: Ethernet Port LEDs

LAN Status	LED 1	LED 2
10 Mbps connection	Off	Off

Table 6: Ethernet Port LEDs (*continued*)

LAN Status	LED 1	LED 2
100 Mbps connection	Green	Off
1000 Mbps connection	Orange	Off
Data is being transferred	Orange, Green, or Off	Blinking
No connection	Off	Off

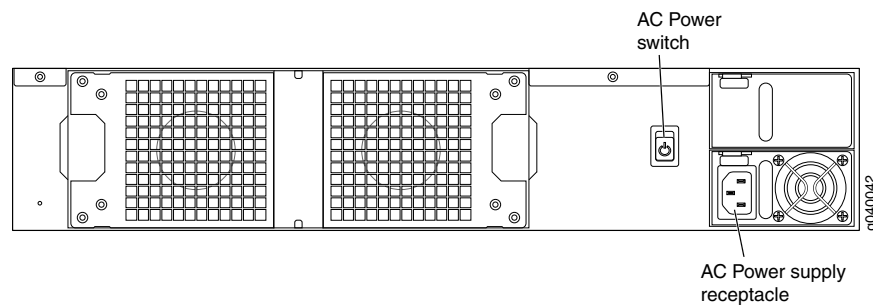
## Installing the NSM3000 Hardware

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

To install NSM3000:

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

Figure 2: Rear Panel of NSM3000



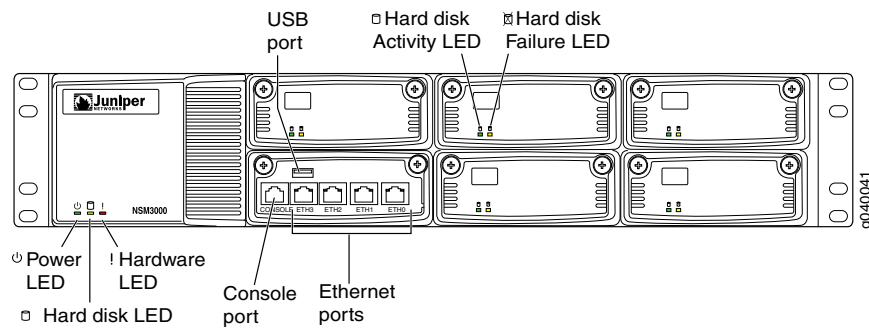
If your NSM appliance contains two power supplies, plug a power cord into each AC receptacle.

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

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

6. Plug the Ethernet cable into the port marked ETH0 on the front panel.

Figure 3: Front Panel of NSM3000



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

This cable was shipped with your NSM3000. If you do not have this cable, use any other null modem serial cable.

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

The green LED below the power button turns on. The NSM3000 hard disk LED turns on whenever the appliance reads data from or writes data to an NSM3000 hard disk.

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

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

## Initial Setup Configuration

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

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

- Boot the NSM Appliance on page 8
- Set Up Your Appliance on page 9

## Boot the NSM Appliance

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

1. Configure a console terminal or terminal emulation utility to use the following serial connection parameters:
  - 9600 bits per second
  - 8-bit no parity (8N1)

- 1 stop bit
  - No flow control
2. Connect the terminal or laptop to the null modem serial cable plugged into the NSM appliance console port.
  3. Turn on the NSM appliance.

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

```
NSMxpress.juniper.net login:
```

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

## Set Up Your Appliance

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

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

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

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

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

```
To configure your system via command line, type:
nsm_setup
```

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

```
[admin@NSMxpress ~]$
```

To complete the setup process using the CLI, go to “CLI Configuration” on page 10. To complete the setup process using the Web interface, go to “Web Interface Configuration” on page 10.

### 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.
2. Enter your password and then press Enter.

```
Juniper NSMXpress OS build 2.105498
NSM 2010.2Kernel 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]
```

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 13 for information about how to install and configure NSM on your NSM appliance from the CLI.

### NSM Appliance Users

An NSM appliance 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 an appliance.

- “admin” user—Logs into the NSM appliance 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 NSM appliance. To return to the “admin” user, enter **exit** at 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 NSM 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 the NSM appliance:

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

2. Open a Web browser and paste the URL into the address text box.
3. Press Enter to open the NSM appliance login page.
4. Enter the admin user name and password and then click Login.
5. See “Configuring NSM from the Web Interface” on page 31 for details about how to install and configure NSM on your NSM 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 appliance from the command-line interface (CLI). It contains the following sections:

- Navigating the Menus on page 13
- Configuring the NSM Software on page 15
- Configuring a Regional Server on page 16
- Configuring the Central Manager on page 21
- Configuring Standard Configuration Options on page 25
- The NSM Appliance Default Restoration on page 29

## Navigating the Menus

---

As you configure NSM on your NSM 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 13
- Using `nsm_setup` on page 14

## 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 leave 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 setup program and later return to it. Follow these steps to return to the NSM appliance setup program. The steps in this procedure assume the NSM appliance is connected to a computer running a terminal emulation program. If not, see “Initial Setup Configuration” on page 8 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 the NSM appliance and wait for the login prompt:

```

Juniper NSMXpress NSM 2010.2Kernel 2.6.9-42.0.8.ELsmp on an i686

NSMXpress.juniper.net logon: admin
Password:
Last Login: Tue May 17 09:43:50 on tty50
Run NSMXpress system setup? [y/N] N

To start system setup manually, type:
nsm_setup

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

[admin@NSMXpress ~]$

```

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

## Configuring the NSM Software

After you log in as an "admin" user, an initial setup script walks you through additional configuration system settings before finalizing the NSM installation. This 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:

```

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

To configure your system via command line, type:
nsm_setup

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

[admin@NSMXpress ~]$

```

Your NSM appliance comes preconfigured as a regional server or a central manager, as described in the following sections:

- Configuring a Regional Server on page 16
- Configuring the Central Manager on page 21

## Configuring a Regional Server

---

For details on using the general setup menu items, see “Navigating the Menus” on page 13.

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 16
- Configuring Custom Settings on page 17

## 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 17
- Configuring Advanced Options on page 19

### 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 “The NSM Appliance Default Restoration” on page 29 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 the NSM appliance 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. NSM appliances support 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 26 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 SecondaryServers.

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]:

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.
- 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 20
- Enabling and Configuring the Statistical Report Server on page 20

### 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 the Statistical Report Server

The following options are available to configure the 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 13.

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 22.
- 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 22
- Configuring Advanced Options on page 24

## Configuring High Availability

To configure high availability (HA), from the NSM Configuration Main menu, enter **4**. The NSM appliance 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 the NSM appliance 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. NSM 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
   or server:/share

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

4> Return to High Availability menu

```

- 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 26 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**. The NSM appliance 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 24.

### 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 through 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 through 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 NSM appliance Settings Menu:

- Changing the Password on page 25
- Setting Interface Options on page 26
- Setting Routing Options on page 27
- Changing the NSM Appliance Hostname on page 27
- Adding DNS Servers on page 27
- Setting the System Time on page 27
- Forwarding Local Status E-mails on page 28
- Updating System Security on page 28
- Saving Setup Options on page 29

## Changing the Password

To change your password:

1. On the NSM appliance 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 NSM appliance Settings menu.

## Setting Interface Options

The NSM appliance 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 appliance 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 appliance 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 appliance Settings menu.

## Setting Routing Options

To set or modify routing options:

1. On the NSM appliance Settings menu, enter **3** at the prompt.
2. Enter one of the following options:
  - **1** to change default gateway options.

Follow the prompts to change the IP address of the default gateway and return to the NSM appliance Settings menu.

- **2** to change the static routing options.

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

## Changing the NSM Appliance Hostname

To change the hostname:

1. On the NSM appliance 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 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 add the DNS servers:

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

## Setting the System Time

You can change time zones or the Network Time Protocol (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 NSM appliance 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 NSM appliance 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 NSM appliance 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 NSM appliance 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 NSM appliance operating system-level patches that protect the system against any future reported security vulnerabilities. The NSM appliance checks for new updates daily by connecting to Juniper Networks.

To manage system security updates:

1. On the NSM appliance 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 NSM appliance version.
  - 4 to set the proxy for security update check.
3. Follow the prompts to manage security updates, and then return to the NSM appliance Settings menu.

## Saving Setup Options

Before you configure the regional server or the central manager, the NSM appliance opens the Apply Change submenu. If you quit out of a menu after making changes, The NSM appliance 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 NSM appliance setup program. After you cancel 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.

## The NSM Appliance Default Restoration

When you reinstall the NSM appliance, it is completely reimaged. No user data remains on the system. If you want to preserve your database, back it up before reinstalling.

To reinstall an NSM appliance, use the following procedure. The steps in the procedure assume the NSM appliance is connected to the computer with a null-modem cable. If not, refer to the section “Initial Setup Configuration” on page 8 for details.

To reinstall the NSM appliance configuration:

1. Turn on the NSM appliance.
2. Press any key while the Booting NSMExpress countdown scrolls through the screen to access the boot menu:

```
Press any key to enter the menu
```

```
Booting NSMExpress  
Booting NSMExpress  
Booting NSMExpress  
Booting NSMExpress  
Booting NSMExpress  
Booting NSMExpress  
in 4 seconds...
```

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

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



**NOTE:** If you have not updated the recovery partition through the Web UI, only the Re-install option (option to install the previous version) is displayed.

---

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 login.

## CHAPTER 3

# Configuring NSM from the Web Interface

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

- Configuring the NSM Software on page 31
- Managing NSM Administration on page 39
- Managing System Administration on page 44
- Maintaining NSM Appliances on page 61
- Troubleshooting on page 63
- Viewing System Information on page 69

## 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 NSM 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 NSM appliance Web interface, you have 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>/administration> URL for your appliance in a Web browser. See “Web Interface Configuration” on page 10 for details.

3. Log in to the Web interface. The **System Info** page opens.
4. Click the **Install NSM Regional Server** link to view the Install NSM Regional Server page (see Figure 4 on page 32) or click the **Install NSM Central Manager** link to view the Install NSM Central Manager page (see Figure 5 on page 33) as the case may be.



NOTE: The “admin” user default username is *admin* and the password is the one you created in Step 6 of “Boot the NSM Appliance” on page 8.

Figure 4: Regional Server Configuration Main Menu

Login: admin

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

## Install NSM Regional Server

**NSM Configuration Main Menu**

**Management**  172.24.68.111

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

**NSM 'super' password**

Password for 'super' user

**NSM License type**  Base Install

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

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

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

Figure 5: Central Manager Configuration Main Menu

5. Enter the primary IP address of your management server for eth0 (the default).  
You can use the default IP address next to the first radio button or select the second radio button and then enter a different IP address. Each IP address you add (in addition to the default IP address) will be available in the drop-down list after you click the second radio button.
6. Enter the NSM superuser password in the top text box, and then reenter it in the text box below it.  
This password must be at least eight characters long and is case-sensitive. This password is used by the NSM superuser (also referred to as the NSM administrator). This user has the highest level of privileges in NSM.
7. Enter the GUI Server one-time password in the top text box, and then reenter it in the text box below it. This password is used to authenticate this NSM server with other NSM servers with which it communicates. Regional servers use this password to authenticate peer servers in an HA configuration and to authenticate the central manager. The central manager uses this password to authenticate its peer server in an HA configuration and any regional servers it manages. NSM servers must have the same GUI Server one-time password, or the authentication will fail.
8. Select the license option. (This option is available only for regional servers.)
  - a. Select **Base Install** to use the built-in limited device license for as many as 25 devices.
  - b. Click **Upload license file** to upload the license file you generated using the Juniper License Management System (LMS), which permits you to manage more than 25 devices. This license file must be located on your local hard drive.

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

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

## Configuring High Availability

To configure high availability (HA) settings:

1. On the NSM Configuration Main Menu, click **Menu** next to High Availability to access HA options. See Figure 6 on page 34.

**Figure 6: High Availability Options**

**Menu: High Availability**

**High Availability**  n  y

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 NSM 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. (Optional) Click **Menu** next to Shared Disk (see Figure 6 on page 34) to configure a shared disk for regional servers (see Figure 7 on page 35) or for central managers (see Figure 8 on page 35).

Figure 7: Shared Disk Options for Regional Servers

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

Figure 8: Shared Disk Options for Central Managers

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

The NSM appliance 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*.

- (Optional) Click **Menu** next to HA Links (see Figure 6 on page 34) to configure the second link in the HA cluster (see Figure 9 on page 35).

Figure 9: HA Links Options

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

Use the options in this menu to set up a redundant link for the HA cluster. If you are going to use a second link, you need to set the IP address for eth1 before configuring this setting (see “Configuring the Network” on page 45 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 as shown below:

Figure 10: Redundant Links

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

- (Optional) Click **Menu** next to HA Advanced Settings (see Figure 6 on page 34) to configure HA advanced settings (see Figure 11 on page 36).

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

Figure 11: HA Advanced Settings

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

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

## Advanced Options

To display the Advanced Options menu, on the NSM Configuration Main Menu, select **Menu** next to Advanced Options. The Advanced Options menu appears as shown in Figure 12 on page 36.

Figure 12: Advanced Options Menu

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

Advanced installation options include:

- **https port for NBI service**—Allows you to configure a port to listen for messages for the NSM API. By default, this value is 8443. You can configure it to any port number from 1025 to 65535.
- **Remote Replication of Database**—Mirrors the daily backup to an external server. You can toggle it on or off. After you turn it on, use the menu options to configure this option.
- **SRS Enabled Options (regional server only)**—Opens a menu to enable and configure Statistical Report Server (SRS). These options enable the NSM appliance 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 6 on page 34) to configure daily backups (see Figure 13 on page 37).

**Figure 13: Remote Replication of Database Options**

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

2. Use the **Remote Replication of Database** option to turn remote replication on (**y**) or off (**n**). The default is off.
3. Use the **Hour of day to Replicate Database** option to start the backup. The valid range (in hours) is 00-23. 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 a central manager.) To configure statistical report server (SRS) settings:

1. On the Advanced Options menu, click **Menu** next to SRS (see Figure 6 on page 34) to open the SRS menu (see Figure 14 on page 38).

Figure 14: SRS Menu

**Menu: SRS**

**SRS**  n  y

Statistical Report Server will be used with this GUI Server

**SRS DB IP**

Database server IP address

**SRS DB Type**  pgsql  pgsql

Database type

**SRS Database Name**  netscreen

Database name

**SRS DB Owner Name**  netscreen

Database user name

**SRS DB Owner Password**

Database password

2. Use the **SRS** options to turn SRS on (**y**) or off (**n**). The default is off. If you turn on this feature, the server is used with the GUI Server.
3. Use the **SRS DB IP** option to enter the IP address for the server on which you have installed the SRS database server.
4. Use the **SRS DB Type** option to select the database type. The values are pgsql (the default), oracle, or mssql.
5. Use the **SRS Database Name** option to enter the name of the SRS database. The default value is netscreen. To enter another name, click the radio button next to the blank text box and enter the name in the text box.
6. Use the **SRS DB Owner Name** option to enter the owner's name of the SRS database. The default value is netscreen. To enter another name, click the radio button next to the blank text box and enter the name in the text box.

7. Use the **SRS DB Owner Password** option to enter the SRS database password. The password requires a minimum of eight characters and is case-sensitive. Reenter the password in the second text box.
8. Click **Submit** to save the options and return to the NSM Configuration Main Menu.

## Installing NSM Software

After you submit all your configuration options, click **Install** to install the NSM software on your NSM 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.

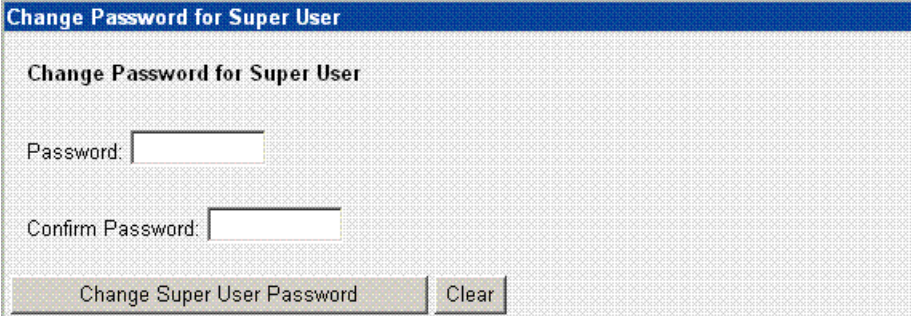
The following sections explain how to use each of the NSM Administration options:

- Changing the Superuser Password on page 39
- Downloading NSM MIBS (Regional Server Only) on page 40
- Exporting Audit Logs on page 40
- Exporting Device Logs (Regional Server Only) on page 40
- Generating Reports (Regional Server Only) on page 41
- Modifying NSM Configuration Files on page 41
- Backing Up the NSM Database on page 42
- Changing the NSM Management IP on page 43
- Scheduling Security Updates on page 43

## Changing the Superuser Password

To change the superuser password, select **NSM Administration > NSM Super User Password**. See Figure 15 on page 39.

Figure 15: Change Superuser Password



**Change Password for Super User**

**Change Password for Super User**

Password:

Confirm Password:

## Downloading NSM MIBS (Regional Server Only)

To download any available MIBs, select **NSM Administration > Download NSM MIBS**, and then click **Download MIB**. See Figure 16 on page 40. This option is not available on the central manager.

Figure 16: Download NSM MIBs



## Exporting Audit Logs

To export audit logs, select **NSM Administration > Export Audit Logs**. See Figure 17 on page 40.

Figure 17: Export Audit Logs



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

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

## Exporting Device Logs (Regional Server Only)

To export device logs, select **NSM Administration > Export Device Logs**. See Figure 18 on page 40. This option is not available on the central manager.

Figure 18: Export Device Logs



## Generating Reports (Regional Server Only)

To generate reports, select **NSM Administration > Generate Reports**. See Figure 19 on page 41. This option is not available on the central manager.

Figure 19: Generate Reports

**Generate Reports**

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

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

User:  Password:   
 Eg: global/super

Schedule Reports:

Minutes:  Hour:  Day:  Month:  Week Day:



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

## Modifying NSM Configuration Files

To manually edit the `GuiSvr.cfg`, `DevSvr.dfg` and `HaSvr.cfg` files, select **NSM Administration > Modify NSM Configuration Files**. The example in Figure 20 on page 42 shows the option to modify the `GuiSvr.cfg` file.

Figure 20: NSM Configuration Files

## NSM Configuration Files

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

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

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

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

setuid.user          nsm
clientId             0
peerGuiSvrId        2
clientOneTimePassword dk2003ns

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

#guiSvrManager.printLevel debug
```

Save



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

### Backing Up the NSM Database

To configure backups of the NSM database, select **NSM Administration > NSM Database Backup** link under NSM Administration. See Figure 21 on page 43.

Figure 21: Database Backup

## Database Backup

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

### Changing the NSM Management IP

To change the IP address of the NSM management server, select **NSM Administration > NSM Management IP** link under NSM Administration. See Figure 22 on page 43.

Figure 22: Change Management IP

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

### Scheduling Security Updates

To schedule security updates, select **NSM Administration > Schedule Security Updates**. See Figure 23 on page 44.

Figure 23: Schedule Security Updates

**Security Update**

**Select Post Action:**

update-devices skip

*Update Devices after Attack* *Select update device action: Skip(skips update of unconnected device)*

User: Password:

Eg: global/super

Schedule Security Updates:

Minutes: Hour: Day: Month: Day: Week

Run Security Update

## Managing System Administration

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

- Rebooting or Shutting Down the NSM Appliance on page 44
- Changing the User Password on page 45
- Configuring the Network on page 45
- Managing RADIUS Servers on page 47
- Monitoring with SNMP on page 50
- Forwarding Syslog Messages on page 53
- Changing the System Time on page 56
- Installing Updates on page 56
- Managing Users on page 57
- Configuring the Web Interface on page 60

### Rebooting or Shutting Down the NSM Appliance

To reboot or shut down the NSM appliance, select **System Administration > Bootup and Shutdown**, and then click either **Reboot System** or **Shutdown System**. See Figure 24 on page 44.

Figure 24: ReBoot or Shut Down

**Bootup and Shutdown**

Reboot System

Shutdown System

## Changing the User Password

To change the user password, select **System Administration > Change User Password**, fill out the form shown in Figure 25 on page 45, and then click **Change**.

Figure 25: Change User Password

**Changing NSMpress user password**

Changing password for admin

Old password

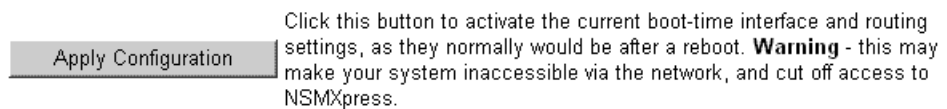
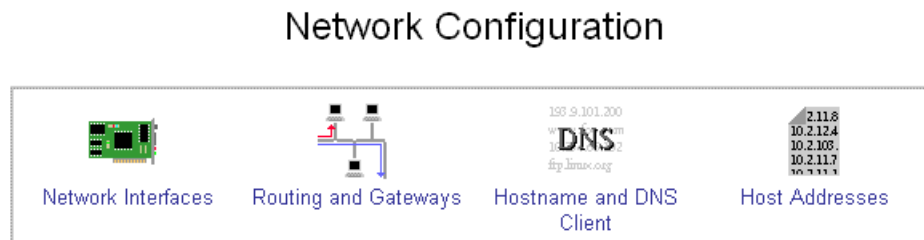
New password

New password (again)

## Configuring the Network

To access options that allow you to configure the network, select **System Administration > Network Configuration**. The Network Configuration window appears as shown in Figure 26 on page 45.

Figure 26: Network Interfaces Options



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

- Network Interfaces on page 45
- Routing and Gateways on page 46
- Hostname and DNS Clients on page 46
- Host Addresses on page 47

### Network Interfaces

Use this option to manage the network interfaces. See Figure 27 on page 46.

Figure 27: Network Interfaces

Module Index

## Network Interfaces

## Interfaces Active Now

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

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

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

De-Activate Selected Interfaces

## Interfaces Activated at Boot Time

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

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

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

Delete Selected Interfaces

Delete and Apply Selected Interfaces

Apply Selected Interfaces

## Routing and Gateways

Use this option to configure and manage routes and gateways. See Figure 28 on page 46.

Figure 28: Routes and Gateways

| Routing configuration activated at boot time                                        |                  |                |                |                |
|-------------------------------------------------------------------------------------|------------------|----------------|----------------|----------------|
| <b>Default routes</b>                                                               |                  |                |                |                |
|                                                                                     | <b>Interface</b> | <b>Gateway</b> |                |                |
|                                                                                     | eth0             | 172.24.68.1    |                |                |
|                                                                                     |                  |                |                |                |
| <b>Act as router?</b> <input type="radio"/> Yes <input checked="" type="radio"/> No |                  |                |                |                |
| <b>Static routes</b>                                                                |                  |                |                |                |
|                                                                                     | <b>Interface</b> | <b>Network</b> | <b>Netmask</b> | <b>Gateway</b> |
|                                                                                     |                  |                |                |                |
| <b>Local routes</b>                                                                 |                  |                |                |                |
|                                                                                     | <b>Interface</b> | <b>Network</b> | <b>Netmask</b> |                |
|                                                                                     |                  |                |                |                |
| <b>Save</b>                                                                         |                  |                |                |                |

## Active Routes

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

## Hostname and DNS Clients

Use this option to configure and manage hostnames and DNS clients. See Figure 29 on page 47.

Figure 29: DNS Client Options

### Host Addresses

Use this option to manage host addresses, See Figure 30 on page 47.

Figure 30: Host Address

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

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

Delete Selected Host Addresses

## Managing RADIUS Servers

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

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



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



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

The following sections explain how to manage a RADIUS server.

- Adding a RADIUS Server on page 48
- Changing the Priority of RADIUS Servers on page 49
- Deleting a RADIUS Server on page 49
- Editing RADIUS Server Parameters on page 49

### Adding a RADIUS Server

To add a RADIUS server:

1. Select **System Administration > RADIUS Management**. The RADIUS Servers dialog box appears listing the RADIUS Servers that have been added. See Figure 31 on page 48.

Figure 31: RADIUS Servers Dialog Box

Radius Servers

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

Add Delete Selected Move Up Move Down Select All

2. Click **Add** to add a RADIUS Server to the WebUI. The Add RADIUS Server dialog box appears. See Figure 32 on page 48.

Figure 32: Add RADIUS Server Dialog Box

Add Radius Server

Add RADIUS Server

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

Add Clear

[← Return to Radius Servers list](#)

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

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

### Changing the Priority of RADIUS Servers

To change the priority of RADIUS servers:

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

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

### Deleting a RADIUS Server

To delete a RADIUS server:

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



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

### Editing RADIUS Server Parameters

To edit the parameters of a RADIUS server:

1. Select **System Administration > RADIUS Management**. The RADIUS Servers dialog box appears listing the RADIUS Servers that have been added.
2. Select the name of the server whose properties you want to edit. The Edit RADIUS Server dialog box appears. See Figure 33 on page 50.

Figure 33: Edit RADIUS Server Dialog Box

Module Index Edit Radius Server

---

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

← [Return to Radius Servers list](#)

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

## Monitoring with SNMP

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

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

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

- SNMP Configuration on page 50
- SNMP System Information on page 51
- SNMP Trap Configuration on page 52

### SNMP Configuration

To configure SNMP:

1. Select **System Administration > SNMP Monitoring**.
2. Select the **SNMP Config** tab, which is shown in Figure 34 on page 51.

Figure 34: Configuring SNMP

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

The password must be at least 8 characters long.

The NSM appliances implement a single username and password, which is effective only for SNMP communication and is not related to any other username and password used on the NSM appliance.

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

### SNMP System Information

To configure SNMP system information:

1. Select **System Administration > SNMP Monitoring**.
2. Select the **System Info** tab, which is shown in Figure 35 on page 51.

Figure 35: Configuring SNMP System Information

3. Enter the following information, with is required for any SNMP-managed device:
  - Contact—Contact information for the appliance.
  - Location—Location of the appliance.

- Description—A brief description of the appliance.
4. Click **Save**.

### SNMP Trap Configuration

To configure SNMP trap conditions:

1. Select **System Administration > SNMP Monitoring**.
2. Select the **SNMP Traps** tab, which is shown in Figure 36 on page 52.

Figure 36: Configuring SNMP Traps

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

3. In the Manager IP field, enter the IP address of the SNMP management server.
4. Select from the following trap conditions:
  - **Disk space low**  
Enter the percentage of free disk space below which SNMP issues a trap.
  - **Memory low**  
Enter the percentage of free memory below which SNMP issues a trap.
  - **CPU high**  
Enter the percentage of CPU use over which SNMP issues a trap.
  - **NSM start/stop**
  - **Admin Logon/Logoff**
  - **External IP unreachable**  
Enter the IP address of the required device.
5. Click **Save**.

## Forwarding Syslog Messages

The NSM appliances provide a simple mechanism for configuring syslog messaging between the NSM 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, the NSM appliance 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 53
- Adding and Configuring Syslog Receivers on page 54
- Editing Syslog Receiver Configurations on page 56
- Deleting Syslog Receivers on page 56

### Viewing Syslog Receivers

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

1. Select **System Administration > Syslog Forwarding**. The Syslog Forwarding window appears. Figure 37 on page 55 shows an example.

### Syslog Forwarding

Select all. | Invert selection. | Add new Receiver

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

Select all. | Invert selection. | Add new Receiver

Delete selected receivers

| NSM Data Sources  |                 |
|-------------------|-----------------|
| GUI Server Log    | Syslog facility |
| fingerprintMPK.D  | user            |
| generateMPK.D     | user            |
| gproGDM.log       | user            |
| guiDaemon.D       | user            |
| license.log       | user            |
| nbiservice.log    | user            |
| pro.mc.log        | user            |
| statusMonitor.D   | user            |
| webproxy.log      | user            |
| xdbservice.log    | user            |
| Device Server Log | Syslog facility |
| datacollector.log | user            |
| ddhnspl.log       | user            |

2. View the configured syslog receivers in the table in the top portion of the window. Table 7 on page 54 describes the fields.

**Table 7: Viewing Syslog Receivers**

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

### Adding and Configuring Syslog Receivers

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

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 37 on page 55.

Figure 37: Configuring a Syslog Receiver

**Syslog Receiver**

**Name:**

**IP:**

**Transport:**  UDP  TCP  SSL

**Data Sources**

**System Logs**

Console messages

Mail log

System updates

**NSM**

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

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

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

- 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.
- In the IP field, Enter the IP address of the syslog receiver.
- In the Transport field, select the type of syslog receiver:
  - Select **UDP** for basic syslog implementations.
  - Select **TCP** for rsyslog or syslog-NG implementations.

- Select **SSL** to create a secure tunnel to a syslog receiver in rsyslog or syslog-NG implementations.
  - In the System Logs section of the Data Sources table, select the sources of data from which system messages will be forwarded to the syslog receiver. These sources can include NSM appliance 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**.

The NSM appliance 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 NSM appliance version.
- Add or modify proxy settings for the Yum server.

## Managing Users

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



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

This topic contains the following sections:

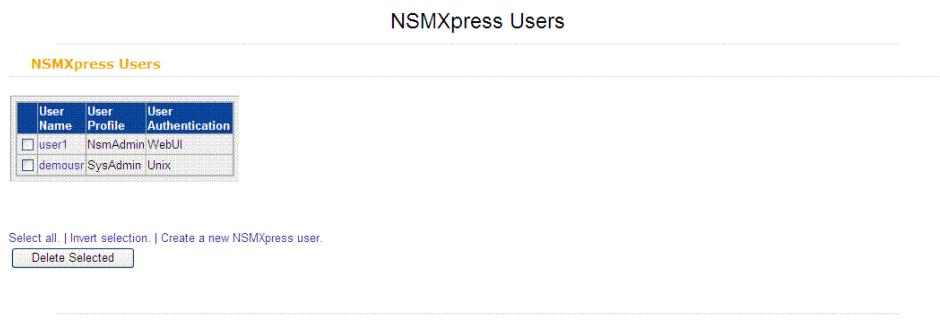
- [Creating New NSM Appliance Users](#) on page 57
- [Deleting a User](#) on page 58
- [Editing User Attributes](#) on page 59
- [Understanding User Profiles](#) on page 59

### Creating New NSM Appliance Users

To create a local OS user:

1. Select **System Administration > User Management**. The NSMxpress Users dialog box appears listing all NSMxpress users. See Figure 38 on page 57.

**Figure 38: NSMxpress Users Dialog Box**



2. Click **Create a new NSMxpress User**. The Create NSMxpress user dialog box appears. See Figure 39 on page 58.

Figure 39: Create NSMXpress User Dialog Box

Module Index Create NSMXpress User

**Create New User**

**Username**

**Password** Unix authentication ▾

**Confirm Password**

**User Profile** NsmAdmin ▾

[← Return to user list](#)

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

To create a WebUI user:

1. Select **System Administration > User Management**. The NSMXpress Users dialog box appears listing all the NSM appliance users. See Figure 40 on page 58.
2. Click **Create a new NSMXpress User**. The Create NSMXpress user dialog box appears.
3. Enter a user name in the **Username** text box.
4. Select **Set to** from the password drop-down list and enter the password you want to set in the password text box.
5. Reenter the password in the **Confirm Password** text box.
6. Select the user profile you want to associate with this user from the **User Profile** drop-down list box.
7. Click **Submit**. The NSMXpress Users dialog box appears with the new NSM appliance user listed.

### Deleting a User

To delete a user:

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



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

### Editing User Attributes

To edit user attributes:

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

### Understanding User Profiles

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

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

When a user logs in, the NSM appliance modules are displayed or hidden based on the user profile and the permissions associated with the profile. For more details about user profiles and permissions, see Table 8 on page 59.

**Table 8: NSM Appliance WebUI User Profiles and Permissions**

| NSM Appliance Modules        | System Administrator | NSM Administrator | Network Operator | Guest User |
|------------------------------|----------------------|-------------------|------------------|------------|
| <b>System Administration</b> |                      |                   |                  |            |
| Bootup and Shutdown          | Yes                  | No                | No               | No         |
| Change User Password         | Yes                  | No                | No               | No         |
| Network Configuration        | Yes                  | No                | No               | No         |
| RADIUS Management            | Yes                  | Yes               | No               | No         |
| SNMP Monitoring              | Yes                  | No                | No               | No         |
| Syslog Forwarding            | Yes                  | No                | No               | No         |
| System Time                  | Yes                  | No                | No               | No         |

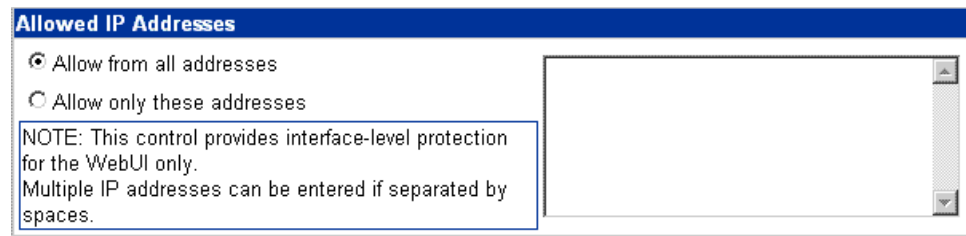
Table 8: NSM Appliance WebUI User Profiles and Permissions (*continued*)

| NSM Appliance Modules          | System Administrator | NSM Administrator | Network Operator | Guest User |
|--------------------------------|----------------------|-------------------|------------------|------------|
| System Update                  | Yes                  | No                | No               | No         |
| User Management                | Yes                  | No                | No               | No         |
| WebUI Configuration            | Yes                  | No                | No               | No         |
| <b>NSM Administration</b>      |                      |                   |                  |            |
| Change NSM Super User Password | Yes                  | Yes               | No               | No         |
| Download NSM MIBs              | Yes                  | Yes               | No               | No         |
| Export Audit Logs              | Yes                  | Yes               | Yes              | No         |
| Export Device Logs             | Yes                  | Yes               | Yes              | No         |
| Generate Reports               | Yes                  | Yes               | Yes              | No         |
| NSM Configuration Files        | Yes                  | Yes               | No               | No         |
| NSM Database Backup            | Yes                  | Yes               | No               | No         |
| NSM Management IP              | Yes                  | Yes               | No               | No         |
| Schedule Security Updates      | Yes                  | Yes               | No               | No         |
| <b>Maintenance</b>             |                      |                   |                  |            |
| System Statistics              | Yes                  | Yes               | Yes              | Yes        |
| <b>Troubleshooting</b>         |                      |                   |                  |            |
| Action Audit Logs              | Yes                  | Yes               | No               | No         |
| Error Logs                     | Yes                  | Yes               | Yes              | No         |
| Network Utilities              | Yes                  | Yes               | Yes              | No         |
| Tech Support                   | Yes                  | Yes               | Yes              | No         |
| System Information             | Yes                  | Yes               | Yes              | Yes        |

## Configuring the Web Interface

To specify which NSM client computers can access the NSM appliance through the Web interface, select **System Administration > WebUI Configuration**. The Allowed IP Addresses window appears as shown in Figure 41 on page 61.

Figure 41: Web Interface Access



## Maintaining NSM Appliances

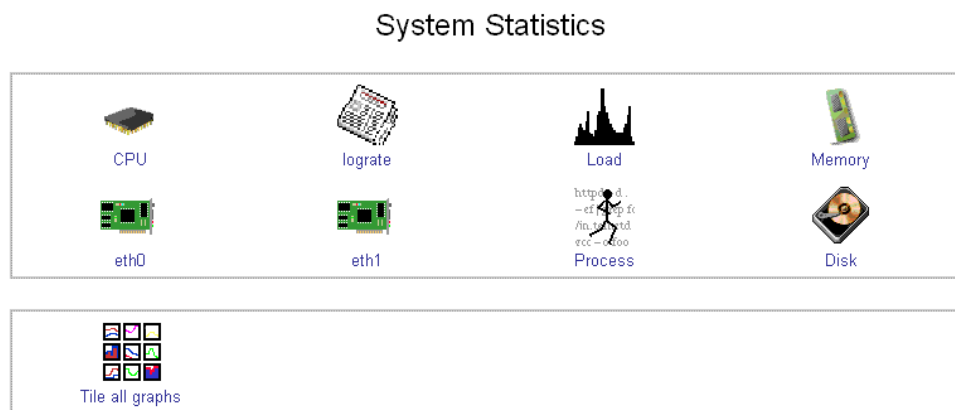
The Maintaining section of the NSM appliance navigation tree allows you to perform the tasks described in the following sections:

- Viewing System Statistics on page 61
- Upgrading the Recovery Partition on page 62

### Viewing System Statistics

To view system statistics, select **System Administration > Maintenance > System Statistics**. The system Statistics window appears as shown in Figure 42 on page 61.

Figure 42: System Statistics



#### CPU

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

#### Log Rate

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

#### CPU Load

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

### Memory Data

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

### Network Data

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

### Process Count

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

### Disk Data

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

### Tile All Graphs

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

## Upgrading the Recovery Partition

The recovery partition contains all files necessary to perform a clean installation of the NSM appliance OS and its applications with default settings. It provides a last-resort recovery mechanism. When the NSM appliance is shipped from the factory, the recovery partition files match the version of the NSM appliance OS with factory default settings.

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

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

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

To upgrade the recovery partition, follow these steps:

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

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

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

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

The Preparation Progress screen shows the progress of the operation.

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

When preparation is completed, the Upgrade window appears.

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

The upgrade process usually takes less than one minute.



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

## Troubleshooting

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

- Auditing User Operations on page 63
- Error Logs on page 65
- Network Utilities on page 66
- Tech Support on page 68

### Auditing User Operations

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

To view Action Audit Logs:

1. Select **Troubleshooting > Action Audit Logs**. The NSMXpress Actions Log dialog box appears. See Figure 43 on page 64.

Figure 43: NSMXpress Actions Dialog Box

NSMXpress Actions Log

Search the NSMXpress log for actions ..

Search

Actions by NSMXpress users

- By any user
- By user | admin
- By any user except | admin

Actions by user profile

- By any profile
- By profile | NsmAdmin
- By any profile except | NsmAdmin

Actions by authentication mechanism

- By any authentication
- By authentication | Unix
- By any authentication except | Unix

Actions in module

- In any module
- In module | Action Audit Logs

Actions on dates

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

2. Select the Action Audit Logs that you want to view:
  - **Actions by NSMXpress Users:** Select the **By any user** check box to select actions by all users. Select the **By user** check box and choose a username from the drop-down list to specify actions by a particular user. Select **By any user except** and choose a username from the drop-down list to exclude actions by a specific user.
  - **Actions by User Profile :** Select the **By any profile** check box to select actions by all user profiles. Select the **By profile** check box and choose a profile from the drop-down list to specify actions by a specific user profile. Select **By any profile except** and choose a profile from the drop-down list to exclude actions by a user profile.
  - **Actions by authentication mechanism:** Select the **By any authentication** check box to select actions by all authentication mechanisms. Select the **By authentication** check box and choose an authentication mechanism from the drop-down list to specify actions by a specific authentication mechanism. Select **By any authentication except** and choose a profile from the drop-down list to exclude actions by an authentication mechanism.
  - **Actions in module:** Select the **In any module** check box to select actions in all modules. Select the **In module** check box and choose a module from the drop-down list to specify actions in a particular module.
  - **Actions on dates:** Select the **At any time** check box to select actions at any time. Select the **For today only** check box to select today's actions. Select the **For yesterday only** check box to select yesterday's actions. Select the **During the last week** check box to select last week's actions. Select the **Between** check box and

enter the start date and end date in the drop-down list to view actions within the specified time period.

3. Click **Search**. The Search Results dialog box appears with the result of your query. See Figure 44 on page 65.

**Figure 44: Search Results Dialog Box**

| Module Index                      |                   | Search Results |              |                     |                |             |       |
|-----------------------------------|-------------------|----------------|--------------|---------------------|----------------|-------------|-------|
| Logged actions on 14/Aug/2009 ... |                   |                |              |                     |                |             |       |
| Action                            | Module            | User           | User profile | User Authentication | Client Address | Date        | Time  |
| Created NSMxpress user demouaz    | User management   | admin          | SysAdmin     | Unix                | 10.206.144.154 | 14/Aug/2009 | 04:11 |
| Created NSMxpress user usez1      | User management   | admin          | SysAdmin     | Unix                | 10.206.144.154 | 14/Aug/2009 | 04:11 |
| Deleted Radius Server thirty-five | Radius Management | shaleen        | SysAdmin     | Radius              | 10.206.146.216 | 14/Aug/2009 | 00:53 |
| Deleted 1 NSMxpress users         | User management   | shaleen        | SysAdmin     | Radius              | 10.206.146.216 | 14/Aug/2009 | 00:52 |
| Added Radius Server thirty-five   | Radius Management | admin          | SysAdmin     | Unix                | 10.206.146.216 | 14/Aug/2009 | 00:39 |
| Created NSMxpress user sanjay     | User management   | admin          | SysAdmin     | Unix                | 10.206.146.216 | 14/Aug/2009 | 00:37 |

[Return to search form](#)

## Error Logs

To review error logs, select **Troubleshooting > Error Logs**. Figure 45 on page 65 shows an example,

**Figure 45: Review Error Logs**

### System Logs

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

To view details of an individual error log, select the file you want to view and click **View**. Figure 46 on page 66 shows sample error log details.

Figure 46: Error Log Detail

Module Index View Logfile

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

Last  lines of Only show lines with text

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

Last  lines of Only show lines with text

## Network Utilities

To access basic network utilities (ping, traceroute, and nslookup) for TCP/IP Networking, select **Troubleshooting > Network Utilities**. These tools also provide an IP subnet calculator. See Figure 47 on page 66.

Figure 47: Network Utilities Options



### Ping

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

Figure 48 on page 66 shows an example.

Figure 48: Ping Utility

Module Index Ping

Help..

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

How many Packets?

Packet Size?

Pattern(s) to send (Hex)?

How many sec between sending each packet?

Pattern(s) to send (Hex)?

#### How Many Packets

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

**Packet Size**

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

**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**

The NSM appliance 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 49 on page 67.

**Figure 49: Traceroute Utility**

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

**Traceroute**

Hostname:

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



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

## Lookup

Use the lookup tool to obtain the IP address from a hostname and the hostname from an IP address (see Figure 50 on page 68). 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 uses the server on which the NSM appliance is installed.

Figure 50: Lookup Utility

Module Index  
Help..

## Lookup

Hostname

Type:

Nameserver:  Default

Timeout?

## IP Subnet Calculator

Use the IP subnet calculator to calculate the netmask for a TCP/IP-network. You can calculate a netmask by class and subnet bits or by the number of hosts (see Figure 51 on page 68). When you calculate a netmask by the number of hosts, the NSM appliance returns the smallest network available.

Figure 51: IP Subnet Calculator

**Calculate Netmask by Class and Bits**

Class:  Subnet Bits:

**Calculate Netmask by Number of Hosts**

Number of Hosts:

## Tech Support

To get contact information for Juniper Networks technical support, select **Troubleshooting > Tech Support**. To help analyze problems, select a detail type in the drop-down list box, and then click **Run Tech-Support Script**. The NSM appliance creates a file you can download and send to Juniper Networks technical support. See Figure 52 on page 69.

Figure 52: Juniper Tech Support

**Tech Support**

Details from Gui, Device and HA servers ▾

Run Tech-Support Script

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

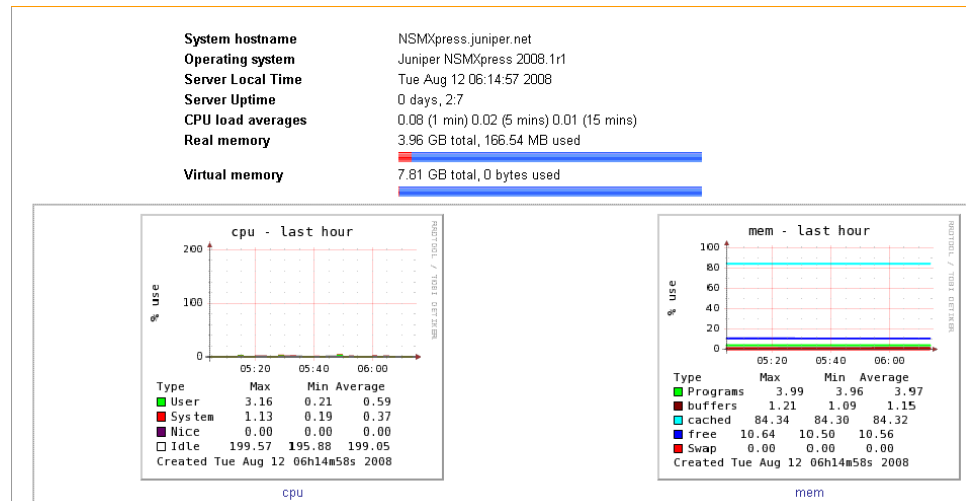
**JTAC PHONE NUMBER:** 1-888-314-JTAC

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

## Viewing System Information

Use the System Information menu item to display information about the server, including CPU load and memory use, as shown in Figure 53 on page 69.

Figure 53: System Information





PART 2

# Appendixes

- NSMXpress LEDs on page 73



## APPENDIX A

# NSMXpress LEDs

This appendix describes the LEDs on the NSMXpress appliance.

- NSMXpress LEDs on page 73

## 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 9 on page 73 describes their states.

**Table 9: NSMXpress LEDs**

| LED     | Color                                 | Condition                                                                                               | Action                    |
|---------|---------------------------------------|---------------------------------------------------------------------------------------------------------|---------------------------|
| TEMP    | Unlit                                 | The temperature is within normal the operating range.                                                   |                           |
|         | Blinking red                          | A fan has failed, but the temperature is still within tolerance and the appliance continues to operate. | Replace the fan.          |
|         | Solid red                             | The temperature has exceeded 120°C. The appliance powers down.                                          | Replace the fan.          |
| PS FAIL | Unlit                                 | Power supplies are functioning normally.                                                                |                           |
|         | Glows red and an audible alarm sounds | A power supply has failed.                                                                              | Replace the power supply. |

**Table 9: NSMXpress LEDs (continued)**

| LED | Color          | Condition               | Action |
|-----|----------------|-------------------------|--------|
| HDD | Unlit          | No hard drive activity. |        |
|     | Blinking amber | Hard drive activity.    |        |
| PWR | Unlit          | The power is off.       |        |
|     | Green          | The power is on.        |        |

## PART 3

# Index

- Index on page 77



# Index

## A

|                            |        |
|----------------------------|--------|
| admin user.....            | 10     |
| Advanced Options menu      |        |
| central manager.....       | 24, 36 |
| regional server.....       | 19, 36 |
| Apply Change menu.....     | 29     |
| audit logs, exporting..... | 40     |

## B

|             |    |
|-------------|----|
| backup..... | 42 |
|-------------|----|

## C

|                                      |        |
|--------------------------------------|--------|
| central manager                      |        |
| configuring with CLI.....            | 21     |
| configuring with Web interface.....  | 31     |
| CLI, configuring NSMXpress from..... | 10, 13 |
| configuration files, editing.....    | 41     |
| console port.....                    | 6      |
| console terminal, configuring.....   | 8      |
| CPU load.....                        | 61     |
| CPU use.....                         | 61     |
| customer support.....                | xviii  |
| contacting JTAC.....                 | xviii  |

## D

|                               |            |
|-------------------------------|------------|
| database                      |            |
| backing up.....               | 42         |
| remote replication of.....    | 20, 24, 37 |
| default gateway               |            |
| address.....                  | 9, 27, 46  |
| default gateway, address..... | 9, 27, 46  |
| defaults, restoring.....      | 29         |
| device logs, exporting.....   | 40         |
| DevSvr.cfg file.....          | 41         |
| disk usage.....               | 62         |
| DMZ.....                      | 4          |
| DNS client.....               | 46         |
| DNS server.....               | 27         |
| documentation                 |            |
| comments on.....              | xviii      |

## E

|                           |        |
|---------------------------|--------|
| e-mail, forwarding.....   | 28     |
| enterprise customers..... | 3      |
| error logs.....           | 65     |
| eth0                      |        |
| activity.....             | 62     |
| configuring.....          | 26     |
| IP address.....           | 9      |
| LED.....                  | 6      |
| subnet mask.....          | 9      |
| eth1                      |        |
| activity.....             | 62     |
| configuring.....          | 26     |
| LED.....                  | 6      |
| Ethernet cable.....       | 6      |
| Ethernet port             |        |
| cabling.....              | 6      |
| configuring.....          | 26     |
| LED.....                  | 6      |
| external clock.....       | 28, 56 |

## G

|                                   |            |
|-----------------------------------|------------|
| GUI Server one-time password..... | 17, 22, 33 |
| GuiSvr.cfg file.....              | 41         |

## H

|                                   |            |
|-----------------------------------|------------|
| HA Advanced Settings menu.....    | 19, 24, 36 |
| HA Links menu.....                | 18, 23, 35 |
| hardware components.....          | 5          |
| hardware installation.....        | 6          |
| HaSvr.cfg file.....               | 41         |
| heartbeat, configuring.....       | 18, 23, 35 |
| high availability                 |            |
| central manager, configuring..... | 22, 34     |
| regional server, configuring..... | 17, 34     |
| High Availability menu            |            |
| central manager.....              | 22         |
| regional server.....              | 17         |
| host address.....                 | 47         |
| hostname.....                     | 27, 46     |

|                                             |            |
|---------------------------------------------|------------|
| <b>I</b>                                    |            |
| interfaces, configuring.....                | 26, 45     |
| IP address, configuring.....                | 9          |
| IP subnet calculator.....                   | 68         |
| <b>L</b>                                    |            |
| LEDs.....                                   | 6          |
| license, NSM.....                           | 17, 33     |
| log rate.....                               | 61         |
| lookup utility.....                         | 68         |
| <b>M</b>                                    |            |
| management IP                               |            |
| central manager.....                        | 22, 33     |
| changing.....                               | 43         |
| regional server.....                        | 17, 33     |
| manuals                                     |            |
| comments on.....                            | xviii      |
| memory usage.....                           | 62         |
| MIBs.....                                   | 40         |
| mounting brackets.....                      | 6          |
| <b>N</b>                                    |            |
| NBI See NSM API                             |            |
| network activity.....                       | 62         |
| network utilities                           |            |
| IP subnet calculator.....                   | 68         |
| lookup.....                                 | 68         |
| ping.....                                   | 66         |
| traceroute.....                             | 67         |
| network, configuring.....                   | 45         |
| northbound interface See NSM API            |            |
| NSM                                         |            |
| configuration files, editing.....           | 41         |
| installing.....                             | 39         |
| updating.....                               | 56         |
| NSM API                                     |            |
| port for central manager.....               | 24         |
| port for regional server.....               | 19, 37     |
| NSM appliances Settings menu.....           | 25         |
| NSM Configuration Main Menu                 |            |
| central manager.....                        | 21         |
| regional server.....                        | 16         |
| NSM license.....                            | 17, 33     |
| nsm user.....                               | 10         |
| nsm_setup utility.....                      | 14         |
| NTP server.....                             | 28, 56     |
| null modem serial cable.....                | 6          |
| <b>P</b>                                    |            |
| password                                    |            |
| admin user.....                             | 25         |
| GUI server, one-time.....                   | 17, 22, 33 |
| heartbeat.....                              | 18, 23, 34 |
| NSM, central manager.....                   | 22         |
| super user, central manager.....            | 33, 39     |
| super user, regional server.....            | 17, 33, 39 |
| user.....                                   | 45         |
| ping utility.....                           | 66         |
| ports, required by NSMExpress.....          | 4          |
| power cord.....                             | 6          |
| primary server, configuring.....            | 18, 23, 34 |
| process count.....                          | 62         |
| <b>R</b>                                    |            |
| reboot.....                                 | 44         |
| Recovery Partition                          |            |
| preparing.....                              | 63         |
| upgrading.....                              | 62         |
| regional server                             |            |
| configuring with CLI.....                   | 16         |
| configuring with Web interface.....         | 31         |
| custom settings.....                        | 17         |
| typical settings, configuring.....          | 16         |
| reinstallation.....                         | 29         |
| Remote Replication of Database menu.....    | 20, 24, 37 |
| reports.....                                | 41         |
| root user.....                              | 10         |
| routing                                     |            |
| default gateway.....                        | 27, 46     |
| static.....                                 | 27, 46     |
| <b>S</b>                                    |            |
| secondary server, configuring.....          | 18, 23, 34 |
| security, updating.....                     | 28, 43     |
| Shared Disk menu.....                       | 18, 23, 34 |
| shutdown.....                               | 44         |
| SNMP                                        |            |
| authentication.....                         | 50         |
| configuring.....                            | 50         |
| monitoring NSM appliances with.....         | 50         |
| system information for.....                 | 51         |
| trap configuration.....                     | 52         |
| SRS See Statistical Report Server           |            |
| SSH.....                                    | 5          |
| static routing.....                         | 27, 46     |
| Statistical Report Server menu.....         | 20, 38     |
| Statistical Report Server, configuring..... | 20, 38     |

---

|                                          |        |
|------------------------------------------|--------|
| subnet calculator.....                   | 68     |
| subnet mask, configuring.....            | 9      |
| sudo su - nsm.....                       | 10     |
| support, technical See technical support |        |
| syslog                                   |        |
| forwarding.....                          | 53     |
| receivers, adding.....                   | 54     |
| receivers, configuring.....              | 54     |
| receivers, deleting.....                 | 56     |
| receivers, editing.....                  | 56     |
| receivers, viewing.....                  | 53     |
| system information.....                  | 69     |
| system logs.....                         | 65     |
| system statistics.....                   | 61     |
| system time.....                         | 27, 56 |
| <br>                                     |        |
| <b>T</b>                                 |        |
| technical support.....                   | 68     |
| contacting JTAC.....                     | xviii  |
| tiling.....                              | 62     |
| time zone.....                           | 28, 56 |
| time, setting.....                       | 27, 56 |
| traceroute utility.....                  | 67     |
| trap conditions, SNMP.....               | 52     |
| troubleshooting.....                     | 63     |
| <br>                                     |        |
| <b>U</b>                                 |        |
| URL, Web interface.....                  | 11     |
| user                                     |        |
| admin, nsm, root.....                    | 10     |
| <br>                                     |        |
| <b>W</b>                                 |        |
| Web interface                            |        |
| configuring.....                         | 60     |
| login URL.....                           | 11     |
| Web interface configuration              |        |
| configuration.....                       | 10     |
| Web login.....                           | 11     |
| <br>                                     |        |
| <b>Y</b>                                 |        |
| Yum server.....                          | 57     |

