



Intrusion Detection and Prevention IDP200, IDP600, IDP1100

Installation Guide

Release 5.0
May 2009

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

Copyright Notice

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.

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.

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Copyright © 2009 Juniper Networks, Inc. All rights reserved.

FCC Statement

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

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

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

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

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device and may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

U.S. Government Rights

Commercial software and commercial software documentation: This documentation is commercial computer software documentation and the products (whether hardware or software) covered by this documentation are or contain commercial computer software. Government users are subject to the Juniper Networks, Inc. standard end user license agreement and any applicable provisions of the FAR and its supplements. No further rights are granted.

Products (whether hardware or software) covered by, and information contained in, this documentation are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical, biological weapons end uses or end users, whether direct or indirect, are strictly prohibited. Export or re-export to countries subject to U.S. embargo or to entities identified on US export exclusion lists, including, but not limited to, the denied persons and specially designated national lists, is strictly prohibited.

Disclaimer

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

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

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 Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and 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, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller. "Embedded Software" means Software which Juniper has embedded in the Juniper 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 the 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 software on multiple computers requires multiple licenses, regardless of whether such computers 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 3D-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 3D-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 the Embedded Software on non-Juniper equipment; (j) use the 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 for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

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 are and will be in the English language)).

Table of Contents

	About This Guide	xiii
	Objectives	xiii
	Audience	xiii
	Conventions	xiii
	Documentation	xiv
	Requesting Technical Support	xvi
	Self-Help Online Tools and Resources	xvi
	Opening a Case with JTAC	xvi
Chapter 1	Hardware and Software Overview	1
	Hardware Overview	1
	IDP Models Overview	1
	IDP200	2
	IDP600C	2
	IDP600F	2
	IDP1100C	3
	IDP1100F	3
	Device LEDs	3
	Serial Console Port	4
	Management Interface Port	4
	HA Interface Port	5
	Traffic Interface Ports	6
	Disk Drives	7
	Power Supplies	8
	Fans	9
	Software Overview	9
	On-Box Management Software	9
	Network and Security Manager	10
	J-Security Center Updates Overview	11
Chapter 2	Installation Overview	13
	Basic Steps	13
	Before You Begin	14
Chapter 3	Installing the Appliance to Your Equipment Rack and Connecting Power	15
	Installing the Device in Your Equipment Rack	15
	Mounting Kits	15
	Required Tools	16
	Mounting Using Midmount Brackets	16
	Mounting to Equipment Rack Rails	17
	Connecting Power	17

Chapter 4	Performing the Initial Network Configuration and Licensing Tasks	19
	Performing the Initial Configuration.....	19
	Recommended Steps.....	19
	Getting Started with the EasyConfig Wizard (Serial Console Port)	20
	Getting Started with the QuickStart Wizard (Management Port)	22
	Getting Started with the ACM Wizard (Management Port)	23
	Installing the Product License Key.....	23
Chapter 5	Connecting the IDP Traffic Interfaces to Your Network and Verifying Traffic Flow	25
	Connecting Interfaces to Your Network.....	25
	Deploying Virtual Routers in the Network Path.....	25
	Interface Port Guidelines	26
	Cable Guidelines for Copper Ports	26
	Connecting Devices That Support Auto-MDIX	27
	Connecting Devices That Do Not Support Auto-MDIX	27
	Connecting Devices to Support Internal Bypass	27
	Connecting and Disconnecting Fiber Cables	27
	Verifying Traffic Flow.....	28
Chapter 6	Adding the IDP Device to NSM	29
	Reviewing Compatibility with NSM	29
	Adding the IDP Device to NSM.....	29
	Checking Device Status	33
Chapter 7	Updating Software	35
	Upgrade Paths.....	35
	Updating IDP Software (NSM Procedure)	35
	Loading a Software Image in NSM	35
	Pushing Software to IDP Devices	36
	Upgrading IDP Software (CLI Procedure).....	37
	Next Steps	37
Chapter 8	Reimaging the IDP Appliance	39
	Reimaging the IDP Appliance.....	39
Chapter 9	Installing Field Replaceable Units	41
	Replacing a Power Supply	41
	Replacing a Hard Drive	43
Appendix A	Specifications	49
	IDP200 Technical Specifications	49
	IDP600 Technical Specifications	51
	IDP1100 Technical Specifications	52
	Safety Compliance	54
	EMI Compliance.....	54
	Immunity	54
Appendix B	Common Criteria EAL2 Compliance	55
	Guidance for Personnel	55

Guidance for Physical Protection.....56

Index.....57

List of Figures

Figure 1: IDP200 Front Panel	2
Figure 2: IDP600C Front Panel	2
Figure 3: IDP600F Front Panel	3
Figure 4: IDP1100C Front Panel	3
Figure 5: IDP 1100F Front Panel	3
Figure 6: System Status LEDs	4
Figure 7: Management Port LEDs	5
Figure 8: HA Port LEDs	6
Figure 9: Copper and Fiber Ports with LEDs	7
Figure 10: Tiers in the Central Management System	11
Figure 11: 1-RU Midmount Bracket	16
Figure 12: 2-RU Midmount Bracket	16
Figure 13: Rail with Hinged Rear Bracket	17
Figure 14: Begin Add Device Procedure	30
Figure 15: Add Device Wizard - Connection Settings	30
Figure 16: Add Device Wizard - Verification Settings	31
Figure 17: Add Device Wizard - Retrieved Settings	32
Figure 18: Add Device Wizard - Adding the Device	32
Figure 19: Add Device Wizard - Importing the Device	32
Figure 20: Viewing Device Status	33
Figure 21: Power Supply Handles in Open and Closed Positions	42
Figure 22: Power Supply Partially Removed	42
Figure 23: Hard Drive Latch in Open Position, Handle Released	44
Figure 24: Hard Drive Handle Down	44
Figure 25: Drive Partially Removed	45
Figure 26: Drive Partially Inserted	46
Figure 27: Hard Drive Latch in Closed Position	46

List of Tables

Table 1:	Notice Icons.....	xiii
Table 2:	Text Conventions.....	xiv
Table 3:	CLI Conventions.....	xiv
Table 4:	GUI Conventions.....	xiv
Table 5:	System Status LED States.....	4
Table 6:	Management Port LEDs	5
Table 7:	HA Port LEDs.....	6
Table 8:	Copper Port LEDs	7
Table 9:	Fiber Port LEDs (IDP 600F, 1100F)	7
Table 10:	Hard Drives and CD-ROM Drives	8
Table 11:	Hard Drive and CD-ROM Drive Status LEDs.....	8
Table 12:	Power Supplies	8
Table 13:	Power Supply Status LED	9
Table 14:	IDP On-Box Utilities	9
Table 15:	Rack Mounting Kits by Model	15
Table 16:	Getting Started Configuration Tools	20
Table 17:	Interface Connection Guidelines	26
Table 18:	IDP200 Physical Specifications	49
Table 19:	IDP200 AC Power Specifications.....	49
Table 20:	IDP200 Power Cord Specifications.....	50
Table 21:	IDP200 Environmental Specifications.....	50
Table 22:	IDP200 Heat Dissipation Guidelines.....	50
Table 23:	IDP600 Physical Specifications	51
Table 24:	IDP600 AC Power Specifications.....	51
Table 25:	IDP600 Power Cord Specifications.....	51
Table 26:	IDP600 Environmental Specifications.....	51
Table 27:	IDP600C Heat Dissipation Guidelines	52
Table 28:	IDP600F Heat Dissipation Guidelines.....	52
Table 29:	IDP1100 Physical Specifications	52
Table 30:	IDP1100 AC Power Specifications.....	52
Table 31:	IDP1100 Power Cord Specifications.....	53
Table 32:	IDP1100 Environmental Specifications	53
Table 33:	IDP1100C Heat Dissipation Guidelines	53
Table 34:	IDP1100C Heat Dissipation Guidelines	53

About This Guide

This guide explains how to install, configure, update, and service a Juniper Networks Intrusion Detection and Prevention (IDP) device.

This preface has the following topics:

- Objectives on page xiii
- Audience on page xiii
- Conventions on page xiii
- Documentation on page xiv
- Requesting Technical Support on page xvi

Objectives

This guide explains how to install, configure, update, and service an IDP Series Intrusion Detection and Prevention appliance.

Audience

This guide is intended for experienced system and network specialists.

Conventions

The following tables show the conventions used throughout this book. Table 1 defines notice icons; Table 2 defines text conventions; Table 3 defines CLI conventions; and Table 4 defines GUI conventions.

Table 1: Notice Icons



Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates that you may risk losing data or damaging your hardware.

Table 1: Notice Icons (continued)


Icon	Meaning	Description
	Warning	Alerts you to the risk of personal injury.

Table 2: Text Conventions

Convention	Description
Plain sans serif type	Filenames and directory names.
<i>Italics</i>	<ul style="list-style-type: none"> ■ Terms defined in text. ■ Variable elements for which you supply values. ■ Book titles.
+ (plus sign)	Key names linked with a plus sign indicate that you must press two or more keys simultaneously.

Table 3: CLI Conventions

Convention	Description
Bold type	Commands that you enter; command names and options.
Plain sans serif type	<ul style="list-style-type: none"> ■ Filenames and directory names. ■ Code and system output.
<i>Italics</i>	Variables for which you supply values.
[] Square brackets	Elements in square brackets indicate optional keywords or variables.
Pipe symbol	Elements separated by the pipe symbol indicate a choice between mutually exclusive keywords or variables.
{ } Braces	Elements in braces indicate required keywords or variables.

Table 4: GUI Conventions

Convention	Description
> (chevron)	Navigation paths through the UI.
Bold type	User interface elements that you select in a procedure, such as tabs, buttons, and menu options.
<i>Italics</i>	Variables for which you supply values.

Documentation

The IDP documentation set includes the following user documentation:

- **IDP Series Release Notes.** Contains information about what is included in a specific product release: supported features, unsupported features, changed features, known problems, and resolved problems. If the information in the *Release Notes* differs from the information found in the documentation set, follow the *Release Notes*.

- **IDP Detector Engine Release Notes.** Contains information about what is included in a specific IDP detector engine release: new features, changed features, known problems, and resolved problems.
- **Juniper Networks Safety Guide.** Provides guidelines and precautions you should become familiar with before you install Juniper Networks hardware.
- **IDP Installation Guide.** Provides instructions for installing, configuring, updating, and servicing the following models: IDP75, IDP200, IDP250, IDP600, IDP800, IDP1100, and IDP8200.
- **IDP Concepts and Examples Guide.** Explains IDP features and provides examples of how to use the system. It also includes a reference of command-line utilities.
- **IDP Administration Guide.** Provides procedures for completing IDP administration tasks with the Network and Security Manager (NSM) central management program; with the IDP device Appliance Configuration Manager (ACM); and with the IDP device command-line interface (CLI).
- **ACM Online Help.** Available through the Appliance Configuration Manager (ACM). The context-sensitive online help describes how to complete the IDP QuickStart and ACM Wizard pages.
- **IDP Reporter User's Guide.** Describes how to use IDP Reporter. The IDP Reporter features and user interface are similar to the Juniper Networks Application Usage Manager features and user interface. Where IDP Reporter includes application usage and attack data for a single IDP device, the application usage manager can aggregate this data for multiple devices and correlate it with subscriber data obtained from SRC devices.
- **Network and Security Manager Administration Guide.** Describes how to use Network and Security Manager (NSM) to update IDP software, firmware, and the attack object database; how to configure IDP devices; and how to implement security policies and attack objects to protect your network. It also describes how to use Profiler, how to monitor IDP events, and how to view system logs, packet logs, and packet captures.
- **Network and Security Manager Configuring Intrusion Detection and Prevention Devices Guide.** Describes how to configure and manage IDP devices using NSM. This guide also helps in understanding of how to configure basic and advanced NSM functionality, including adding new devices, deploying new device configurations, updating device firmware, viewing log information, and monitoring the status of IDP devices.
- **Network and Security Manager Online Help.** Available through NSM. The online Help provides step-by-step instructions for performing administration tasks.

To download the documentation, go to:

<http://www.juniper.net/techpubs/software/management/idp/>.

Requesting Technical Support

Technical 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, you can access our tools and resources online or open a case with JTAC. JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

For product warranty information, visit <http://www.juniper.net/support/warranty/>.

Self-Help Online Tools and Resources

The Juniper Customer Support Center (CSC) provides the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- 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 your release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://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 Manager: <http://www.juniper.net/customers/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 in the following ways:

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

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

Chapter 1

Hardware and Software Overview

This chapter provides an overview of the Juniper Networks Intrusion Detection and Prevention (IDP) device components.

This chapter includes the following topics:

- Hardware Overview on page 1
- Software Overview on page 9

Hardware Overview

This topic provides an overview of IDP hardware. It includes the following information:

- IDP Models Overview on page 1
- Device LEDs on page 3
- Serial Console Port on page 4
- Management Interface Port on page 4
- HA Interface Port on page 5
- Traffic Interface Ports on page 6
- Disk Drives on page 7
- Power Supplies on page 8

For complete specifications for each model, see Appendix A, “Specifications.”

IDP Models Overview

This topic provides an overview of the following models:

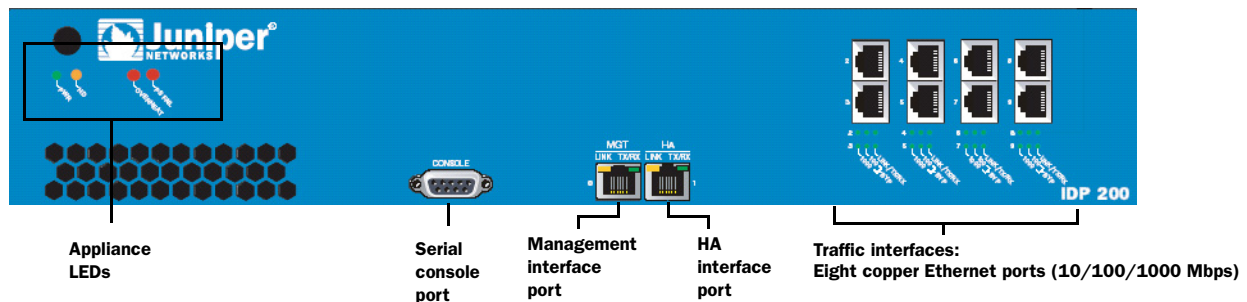
- IDP200 on page 2
- IDP600C on page 2
- IDP600F on page 2

- IDP1100C on page 3
- IDP1100F on page 3

IDP200

The IDP200 appliance is optimal for medium central sites or large branch offices. Figure 1 shows the location of appliance LEDs and ports.

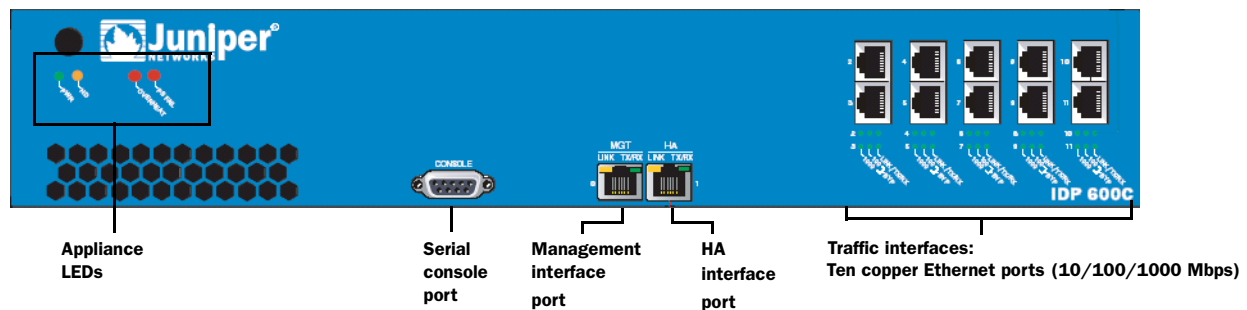
Figure 1: IDP200 Front Panel



IDP600C

The IDP600C appliance is optimal for medium-to-large central sites or high-traffic areas. Figure 2 shows the location of appliance LEDs and ports.

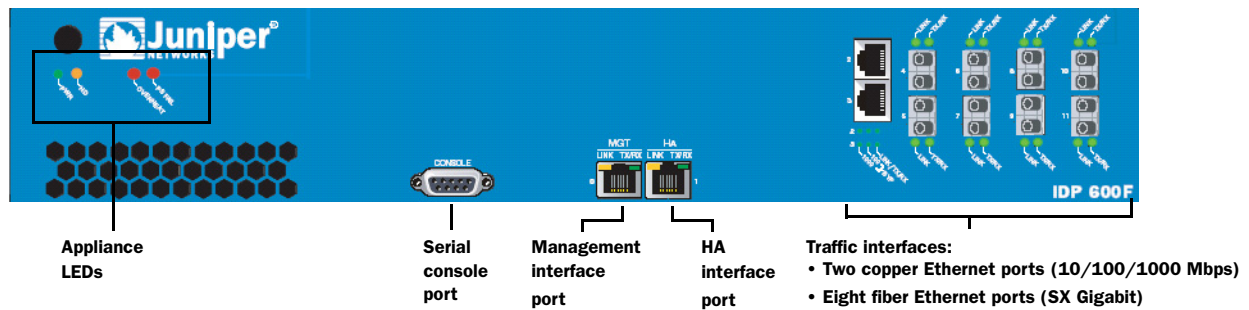
Figure 2: IDP600C Front Panel



IDP600F

The IDP600F appliance is optimal for medium-to-large central sites or high-traffic areas. Figure 3 shows the location of appliance LEDs and ports.

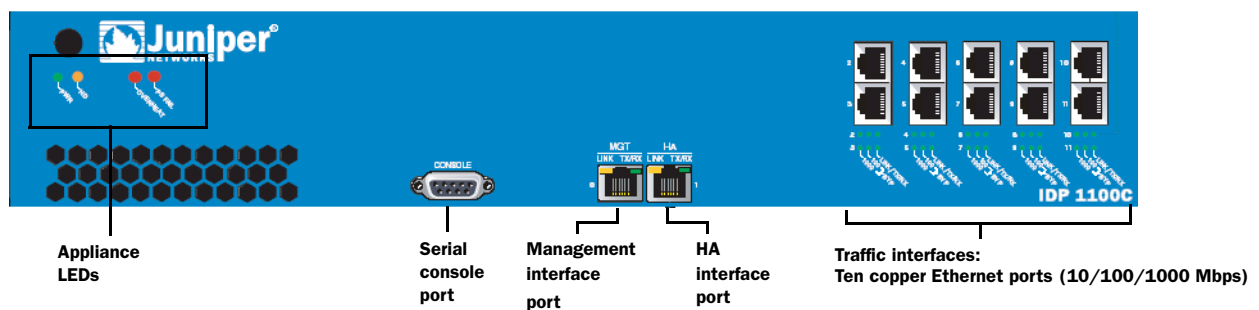
Figure 3: IDP600F Front Panel



IDP1100C

The IDP1100C appliance is optimal for large central sites or high-traffic areas. Figure 4 shows the location of appliance LEDs and ports.

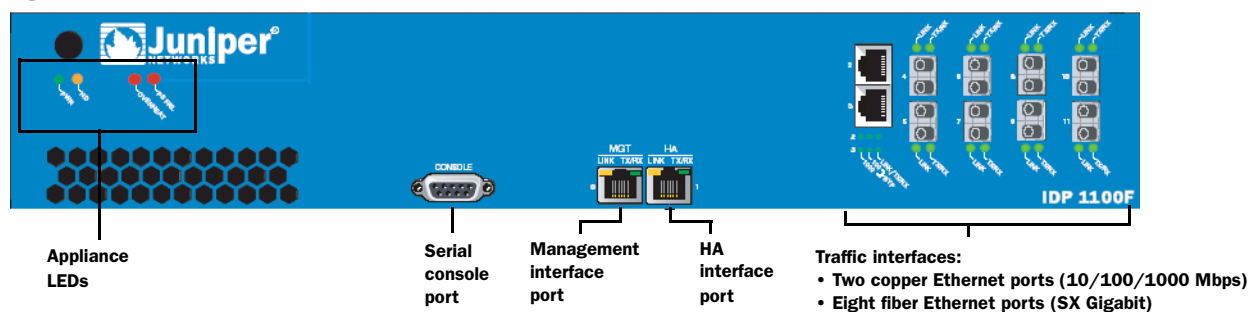
Figure 4: IDP1100C Front Panel



IDP1100F

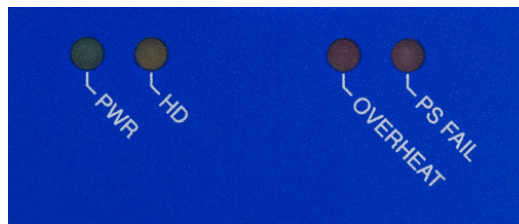
The IDP1100F appliance is optimal for large central sites or high-traffic areas. Figure 5 shows the location of appliance LEDs and ports.

Figure 5: IDP 1100F Front Panel



Device LEDs

Figure 6 shows system status LEDs. Table 5 on page 4 describes LED states.

Figure 6: System Status LEDs**Table 5: System Status LED States**

System Status LED	State	Description
PWR	Solid green	System is powered on.
	Off	System is powered off.
HD	Flashing amber	Hard disk is active.
	Off	Hard drive has no activity.
OVERHEAT	Glows red	Fan failure or the system is overheating.
	Off	System is functioning at a normal temperature.
PS FAIL	Glows red	One of the power supplies has failed or is unplugged.
	Off	Power supplies are operating normally.

Serial Console Port

The console serial port provides access, through a DB-9 serial port, to the command-line interface (CLI).

Management Interface Port

This management port is a 10/100/1000 Mbps Ethernet port. Use the port as a dedicated management port, connecting the device to a switch accessible by your management subnet.

The IP address you assign the management port is the IP address you use to connect to the Appliance Configuration Manager (ACM) when you initially configure the device. It is also the address the Network and Security Manager (NSM) uses to connect to the device.

Figure 7 shows the location of LEDs on the management interface port. Table 6 describes management port LEDs.

Figure 7: Management Port LEDs



Table 6: Management Port LEDs

LED	State	Description
LINK	Glows orange	Connection is 1000 Mbps.
	Glows green	Connection is 100 Mbps.
	Off	If LINK indicates activity, TX/RX off indicates connection is 10 Mbps. If LINK indicates no activity, TX/RX off indicates no activity as well.
TX/RX	Blinks amber	Activity.
	Off	No activity.

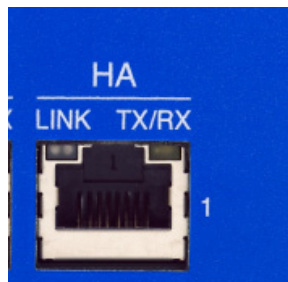
HA Interface Port

The HA interface port is a 10/100/1000 Mbps Ethernet port. The HA interface is a dedicated interface used to share state information among sensors in a cluster.



NOTE: IDP 5.0 does not support high availability.

Figure 8 shows the location of LEDs on the HA interface port. Table 7 describes the HA port LEDs.

Figure 8: HA Port LEDs**Table 7: HA Port LEDs**

LED	State	Description
LINK	Blinks amber	Activity.
	Off	No activity.
TX/RX	Glow orange	Connection is 1000 Mbps.
	Glow green	Connection is 100 Mbps.
	Off	If LINK indicates activity, TX/RX off indicates connection is 10 Mbps. If LINK indicates no activity, TX/RX off indicates no activity as well.

Traffic Interface Ports

Traffic interface ports may be 10/100/1000 Ethernet or Gigabit Ethernet, depending on the IDP system you purchased. Traffic interfaces are named consecutively **eth2**, **eth3**, and so forth.

In IDP deployments, logical pairs of traffic interfaces make up a virtual router. For example, **eth2** and **eth3** belong to the same virtual router. In transparent mode, traffic arrives at one interface and is sent out the other. You can configure interface features per virtual router, such as deployment mode and bypass. For details, see the *IDP Concepts and Examples Guide*.

Figure 9 shows the location of LEDs on traffic interfaces. Table 8 describes copper port LEDs. Table 9 describes fiber port LEDs.

Figure 9: Copper and Fiber Ports with LEDs

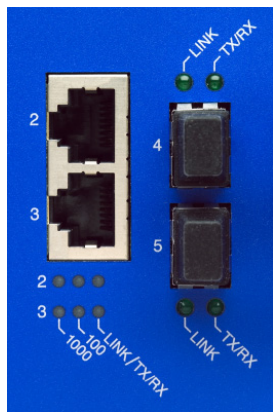


Table 8: Copper Port LEDs

LED	State	Description
1000	Glows green	Connection is 1000 Mbps. If the 100 LED also glows green and the LINK/TX/RX LED is off, the interface is in bypass mode.
	Flashes green	Both the 1000 LED and 100 LED flash when the connection is 10 Mbps.
	Off	No active 1000 Mbps connections.
100	Glows green	Connection is 100 Mbps. If the 1000 LED also glows green and the LINK/TX/RX LED is off, the interface is in bypass mode.
	Flashes green	Both the 1000 LED and 100 LED flash when the connection is 10 Mbps.
	Off	No active 100 Mbps connections.
LINK/TX/RX	Flashes green	Activity.
	Off	No activity.

Table 9: Fiber Port LEDs (IDP 600F, 1100F)

LED	State	Description
LINK	Glows green	Connection is 1 Gbps.
	Off	No active 1 Gbps connections.
TX/RX	Flashes green	Activity on the port.
	Off	No activity on the port.

Disk Drives

Table 10 lists the number of hard drives and CD-ROM drives by model.

Table 10: Hard Drives and CD-ROM Drives

Model	Hard Drives and CD-ROM Drives
200	One internal hard drive. One CD-ROM drive.
600 and 1100	Two externally accessible, hot-swappable, SCSI, RAID 1 mirrored hard drives. One CD-ROM drive.

Table 11 describes hard drive and CD-ROM drive status LEDs. The drive status LEDs are located on the back panel, on the respective drives.

Table 11: Hard Drive and CD-ROM Drive Status LEDs

LED	State	Description
CD-ROM light	Flashes green	Activity.
Hard drive left light (600 and 1100 only)	Glows red	Failure. Note: the system also emits a high-pitch tone if a hard drive has failed.
	Flashes red	Hard drive is being rebuilt. Note: Do not turn the power off, unplug the unit, or remove either drive while the drive is being rebuilt.
	Off	Functioning normally.
Hard drive right light (600 and 1100 only)	Flashes green	Activity.
	Off	No activity.

For procedures on replacing a hard drive, see “Replacing a Hard Drive” on page 43.

Power Supplies

Table 12 lists the power supplies available on each appliance.

Table 12: Power Supplies

Model	Power Supplies
200	One removable power supply. Empty bay for second, optional power supply.
600 and 1100	Two removable, hot-swappable power supplies.

For procedures on replacing a power supply, see “Replacing a Power Supply” on page 41.

Table 13 describes the power supply status LED. The power supply status LED is located on the back panel, above the plug socket.

Table 13: Power Supply Status LED

LED State	Description
Glows amber	Power supply is receiving power.
Glows green	Power supply is powering the unit.
Note: If a power supply has failed or is not receiving power, the system emits a high-pitched tone.	

Fans

When the system is cool, device fans spin at a slower speed to reduce noise and save energy. As the system heats up, the fans run at a faster speed.

In the event of fan failure, the device fault LED blinks and the remaining fan or fans run at full speed until the failed fan is replaced.

Software Overview

This topic provides an overview of IDP software. It includes the following information:

- On-Box Management Software on page 9
- Network and Security Manager on page 10
- J-Security Center Updates Overview on page 11

On-Box Management Software

You use on-box management software to get the device up and running in the desired deployment mode, to configure device interfaces, and to establish communication with Network and Security Manager (NSM). You can also use on-box utilities to manage device processes or generate on-box reports.

Table 14 summarizes the IDP on-box management software and utilities.

Table 14: IDP On-Box Utilities

Software	Usage
EasyConfig	<p>When you install a new device, you can use the EasyConfig script to assign the device an IP address and initialize a simple configuration.</p> <p>To run the EasyConfig script, connect to the serial port console. For details, see “If your model has redundant power supplies, repeat the previous steps to connect the second power supply.” on page 18.</p>
QuickStart	<p>When you install a new device, you can use QuickStart to deploy the device in sniffer or transparent mode with a default configuration.</p> <p>To access QuickStart, connect to the management interface and open the QuickStart URL in your browser. For details, see “If your model has redundant power supplies, repeat the previous steps to connect the second power supply.” on page 18.</p>

Table 14: IDP On-Box Utilities (continued)

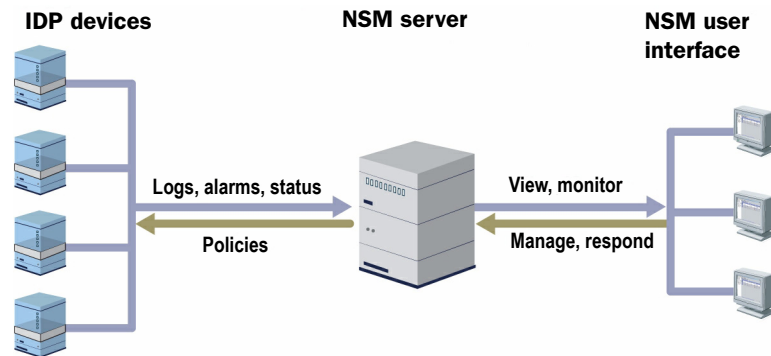
Software	Usage
ACM	<p>When you install a new device, you can use ACM to configure host information, network settings, and virtual router features, such as deployment mode and bypass.</p> <p>You also use ACM to reconfigure the device whenever you want to change deployment modes or traffic interface settings.</p> <p>To access ACM, connect to the management interface and open the ACM URL in your browser. For details, see “If your model has redundant power supplies, repeat the previous steps to connect the second power supply.” on page 18.</p>
scio utility	<p>You can use the scio utility to get or set device configuration information.</p> <p>To access the scio utility, make an SSH connection to the management interface as the user admin and then switch to the user root. For command syntax, see the <i>IDP Concepts and Examples Guide</i>.</p>
idp.sh utility	<p>You can use the idp.sh utility to start, stop, or get status information on device processes.</p> <p>To access the idp.sh utility, make an SSH connection to the management interface as the user admin and then switch to the user root. For command syntax, see the <i>IDP Concepts and Examples Guide</i>.</p>
sctop utility	<p>You can use the sctop utility to monitor connection tables and view status.</p> <p>To access the sctop utility, make an SSH connection to the management interface as the user admin and then switch to the user root. For command syntax, see the <i>IDP Concepts and Examples Guide</i>.</p>
bypassStatus utility	<p>You can use the bypassStatus utility to display settings for the daemon that monitors traffic interface NIC state. The command also displays the NIC state for all such interfaces.</p> <p>To access the bypassStatus utility, make an SSH connection to the management interface as the user admin and then switch to the user root. For command syntax, see the <i>IDP Concepts and Examples Guide</i>.</p>

Network and Security Manager

Juniper Networks Network and Security Manager (NSM) is a central management server capable of managing hundreds of IDP Series appliances and other Juniper Networks devices, such as ScreenOS firewalls, SA Series devices, and IC Series devices. You typically deploy NSM in a management subnet accessible to NSM-managed devices.

Figure 10 illustrates the flow of information between the tiers of the central management solution: the NSM user interface, the NSM server, and IDP devices.

Figure 10: Tiers in the Central Management System



The IDP configuration, security policies, attack objects, and log records are stored in NSM server databases and administered using the NSM user interface. Communication between the NSM server and IDP devices, and between the NSM server and the NSM user interface, is encrypted and authenticated.

For IDP deployments, centralized management provides the following benefits:

- Centralized management of enterprise security policies
- Consolidated logs from different devices in a single repository
- Simplified signature and protocol-anomaly attack-object management
- Centralized management for IDP devices and other network devices
- Role-based administration

For information about adding an IDP device to the NSM device manager, see Chapter 6, “Adding the IDP Device to NSM.”

For complete information about installing NSM and using NSM to administer IDP devices, refer to the *Network and Security Manager Installation Guide* and *Network and Security Manager Administration Guide*.

J-Security Center Updates Overview

The Juniper Networks Security Center (J-Security Center) routinely makes important updates available to IDP security policy components, including updates to the IDP detector engine and the NSM attack database.

The IDP detector engine is a dynamic protocol decoder that includes support for decoding more than 60 protocols and more than 500 service contexts. You should update IDP detector engine when you first install IDP, whenever you upgrade, and whenever alerted to do so by Juniper Networks. You can view release notes for detector engine updates at <http://www.juniper.net/techpubs/software/management/idp/de/>.

The NSM attack database stores data definitions for attack objects. Attack objects are patterns comprising stateful signatures and traffic anomalies. Security policy rules direct the IDP engine to inspect traffic for attack objects. We recommend you schedule automatic updates for the NSM attack database.

For more information about detector engine and attack object updates, see the *IDP Administration Guide*.

Chapter 2

Installation Overview

This chapter includes the following topics:

- Basic Steps on page 13
- Before You Begin on page 14

Basic Steps

To install the device and connect it to your network, follow these basic steps:

1. Read the release notes. Release notes make you aware of supported and unsupported features, known issues, and fixed issues.
2. Become familiar with the safety and security guidelines that pertain to your installation. See “Before You Begin” on page 14.
3. Decide on the physical location for the device. The location depends on your deployment mode, the location of your network devices, and compliance with your company security policy.
4. Install the device into your equipment rack.

Although you can place the device on a desktop for operation, we do not recommend deploying it in this manner.

See “Installing the Device in Your Equipment Rack” on page 15.

5. Connect power cables and power on.

See “Connecting Power” on page 17.

6. Perform the initial configuration steps.

See “Performing the Initial Configuration” on page 19.

7. Install the license key.

See “Installing the Product License Key” on page 23.



NOTE: In these steps, you are instructed to install the product license key before you add the device to NSM. If you install the product license key after you add the device to NSM, you must re-add the device to NSM.

8. Connect the device to your network.

See “Connecting Interfaces to Your Network” on page 25.

9. Verify connectivity.

See “Verifying Traffic Flow” on page 28.

10. In NSM, add the IDP device to the NSM device manager.

See Chapter 6, “Adding the IDP Device to NSM.”

11. Upgrade the IDP software to the current release, update the IDP detector engine, and update the NSM attack object database.

See Chapter 7, “Updating Software.”

Before You Begin

The location of the device, the layout of the mounting equipment, and the security of your wiring room are crucial for proper system operation.



CAUTION: To prevent abuse and intrusion by unauthorized personnel, install the device in a secure environment.

Observing the following precautions can prevent shutdowns, equipment failures, and injuries:

- Before installation, always check that the power supply is disconnected from any power source.
- Ensure that the room in which you operate the device has adequate air circulation and that the room temperature does not exceed 104°F (40°C).
- Do not place the device in an equipment-rack frame that blocks an intake or exhaust port. Ensure that enclosed racks have fans and louvered sides.
- Correct these hazardous conditions before any installation: moist or wet floors, leaks, ungrounded or frayed power cables, or missing safety grounds.

If Common Criteria EAL2 Compliance is required, see Appendix B, “Common Criteria EAL2 Compliance.”

For a comprehensive presentation on the precautions you must take to prevent personal injury and damage to the equipment, see the *Juniper Networks Safety Guide*.

Chapter 3

Installing the Appliance to Your Equipment Rack and Connecting Power

This chapter includes the following topics:

- Installing the Device in Your Equipment Rack on page 15
- Connecting Power on page 17

Installing the Device in Your Equipment Rack

This topic describes how to install the device in your equipment rack. It includes the following information:

- Mounting Kits on page 15
- Required Tools on page 16
- Mounting Using Midmount Brackets on page 16
- Mounting to Equipment Rack Rails on page 17

Mounting Kits

Table 15 describes rack mounting hardware included in a standard shipment. If you require additional rack mounting hardware, contact your sales representative for details on rack mounting kits to suit your needs.

Table 15: Rack Mounting Kits by Model

Form Factor	Mounting Kit
1-RU Models:	Your standard shipment includes a single pair of mounting brackets/ears. To install the appliance in a rack: <ul style="list-style-type: none">■ Position the brackets in the front position to front-mount.■ Position the brackets in the middle position to midmount.
2-RU Models	Your standard shipment includes front-mount ears, midmount brackets, and rear-mount brackets to enable you to secure the appliance in your rack.

Required Tools

To complete the mounting procedure, you need the following tools:

- Number 2 Phillips-head screwdriver
- Rack-compatible screws

Mounting Using Midmount Brackets

To mount the device using the midmount brackets in a device rack:

To mount the device using the midmount brackets in a device rack:

1. Attach one rack-mounting bracket to each side of the chassis with the bracket screws.

See Figure 11 and Figure 12.

Figure 11: 1-RU Midmount Bracket



Figure 12: 2-RU Midmount Bracket



2. Place the chassis into position between rack posts in the equipment rack and align the rack-mounting bracket holes with the rack post holes.



CAUTION: Be sure to leave at least two inches of clearance on the sides of each chassis for the cooling air inlet and exhaust ports.

3. Attach the rack-mounting brackets on each chassis to the rack with the appropriate rack screws.
4. For 2-RU models, attach the other midmount brackets to the chassis and the back of the rack to hold the device securely in place.

Mounting to Equipment Rack Rails

To mount the device to equipment rack rails:

1. Attach the rails to each side of the chassis with the bracket screws. Make sure the hinged brackets are at the back of the device. Make sure the rails are positioned so they reach the back of the rack when the device is mounted. See Figure 13.

Figure 13: Rail with Hinged Rear Bracket



2. Rotate the hinges on both rails so that they allow the device to slide into the rack.
3. Slide the chassis and rails into the rack.



CAUTION: Be sure to leave at least two inches of clearance on the sides of each chassis for the cooling air inlet and exhaust ports.

4. Secure the front brackets to the rack.
5. Rotate the rear brackets so they prevent the device from sliding forward.
6. Secure the rear brackets to the rack.

Connecting Power

Power is provided to the device using 90/264 VAC from your facility.

To connect power to your device:

1. Connect the provided power cable to the receptacle on the power supply at the rear of each chassis.

2. Connect the other end of the power cable to the electrical outlet.
3. If your model has redundant power supplies, repeat the previous steps to connect the second power supply.



NOTE: If your model has redundant power supplies, you have the option of connecting one or both. For greater reliability, consider connecting power supplies to different circuits. The appliance is completely operational with one power supply connected. However, if you connect only one, the PS FAIL warning light illuminates and the appliance emits a warning tone.

Chapter 4

Performing the Initial Network Configuration and Licensing Tasks

This chapter includes the following topics:

- Performing the Initial Configuration on page 19
- Installing the Product License Key on page 23

Performing the Initial Configuration

This topic describes how to perform the initial configuration.

This topic includes the following information:

- Recommended Steps on page 19
- Getting Started with the EasyConfig Wizard (Serial Console Port) on page 20
- Getting Started with the QuickStart Wizard (Management Port) on page 22
- Getting Started with the ACM Wizard (Management Port) on page 23

Recommended Steps

We recommend you take the following steps to perform the initial configuration:

1. In the machine room, connect your laptop to the serial port and run the EasyConfig script to assign the management interface an IP address you can reach from your subnet. See “Getting Started with the EasyConfig Wizard (Serial Console Port)” on page 20.
2. From your desk, run the ACM wizard from your Web browser. See “Getting Started with the ACM Wizard (Management Port)” on page 23. Be sure to change the default passwords.

In some circumstances, you might not be able to use the serial console or might prefer to get started with a simple configuration for limited purposes. For these cases, we support alternative methods for getting started. Table 16 summarizes getting started configuration tools.

Table 16: Getting Started Configuration Tools

Getting Started Tool	You Specify:	Defaults Applied:
EasyConfig wizard (Serial port)	<ul style="list-style-type: none"> ■ One deployment mode for all virtual routers (sniffer or transparent) ■ Management interface IP address and netmask ■ Default route ■ Time zone, date, and time 	<ul style="list-style-type: none"> ■ Root password: abc123 ■ Fully qualified domain name: Blank ■ High availability mode: Disabled ■ RADIUS support: Disabled ■ Network interfaces: Auto-negotiate speed/duplex ■ DNS: Disabled ■ NTP: Disabled ■ SSH on management port: Enabled ■ Start the ACM process when the device starts up: Enabled
QuickStart wizard (Management port)	Same as EasyConfig Wizard.	Same as EasyConfig Wizard.
ACM wizard (Management port)	<ul style="list-style-type: none"> ■ Passwords for root and admin ■ Fully qualified domain name ■ Management interface IP address and netmask ■ High availability options and configuration ■ Traffic interface configuration (speed/duplex, route table) ■ Virtual routers, including deployment mode and bypass settings ■ Peer port modulator (PPM) ■ Layer 2 bypass (pass-through) ■ Network services (DNS, NTP, RADIUS, SSH) ■ ACM access ■ NSM connection information ■ One-time password (OTP) for interoperability with Juniper Networks Secure Access and Infranet Controller devices 	

Getting Started with the EasyConfig Wizard (Serial Console Port)

We recommend you get started by running the EasyConfig wizard to assign an IP address to the management interface. Then, you can access the ACM Wizard from a remote location to complete the device configuration.

To perform the initial configuration with the EasyConfig wizard:

1. Connect one end of the provided RJ-45 null modem serial cable to the serial console port located on the front of the device chassis.

2. Connect the other end of the cable to the serial port of your laptop.
3. Open a terminal emulation package such as Microsoft Windows HyperTerminal or XModem. The settings for the software should be as follows:
 - 9600 bps
 - 8 data bits
 - No parity generation or checking
 - 1 stop bit
 - No flow control
 - The serial port number where you connected the cable
4. Turn on the device.

If nothing appears in the terminal window, press Enter to display the boot messages.
5. Log into the device as **root** with the default password (abc123).



NOTE: After you have completed the initial configuration, we recommend highly that you use ACM to change the default password. See “Getting Started with the ACM Wizard (Management Port)” on page 23.

The EasyConfig script runs automatically. The following text appears:

```
Configuring the deployment mode...
The currently supported deployment modes in EasyConfig are the following,
    1. Sniffer <default>
    2. Inline transparent
Choose the deployment mode? [1]
```

6. Press **1** or **2**, depending on which mode you want to use, and then press Enter.

The following text appears:

```
Configuring Management interface...
The management interface is currently configured as:
    IP: 192.168.1.1
    Mask: 255.255.255.0
What IP address do you want to configure for the management interface?
[192.168.1.1]
```

7. Type an IP address and press Enter.

The following text appears:

```
What netmask do you want to configure for the management interface?
[255.255.255.0]
```

8. Type your netmask and press Enter.

The system configures your interfaces. The following text appears:

```
Configuring default route...
The current default route is: X.X.X.X
Do you want to change the default route? (y/n) [n]
```

9. Type **Y**, and then press Enter.

The following text appears:

```
What IP address do you want to configure as default route? [X.X.X.X]
```

10. Type your default route (gateway address) and press Enter.

The system asks if you want to change the system time.

```
Configuring system time...
Currently configured time is Wed Jan 18 16:32:32 PST 2006
```

```
Do you want to change the system time? (y/n) [n]
```

11. Type **N** if the time is correct. If the time is not correct, type **Y** and follow the prompts to change the system time.

Configuration of the management port is now complete. EasyConfig does not run the next time you log into the device.

Getting Started with the QuickStart Wizard (Management Port)

If you cannot connect to the serial port, you can run the QuickStart wizard from the management port to assign an IP address to the management interface.

To get started with the QuickStart wizard:

1. Connect one end of an Ethernet cable to the management interface port and the other end to the Ethernet port of your laptop.
2. On your laptop, open a Web browser.
3. In the browser Address or Location box, enter **https://192.168.1.1**.



NOTE: ACM access uses SSL, so you must type **https://** and not **http://**.

4. Log in as **root** with the default password (abc123).



NOTE: After you have completed the initial configuration, we recommend highly that you use ACM to change the default password. See “Getting Started with the ACM Wizard (Management Port)” on page 23.

5. Click **QuickStart** to start the QuickStart wizard. Complete the wizard steps as described in the online Help.

If you prefer, you can click **ACM** instead and run the ACM wizard at this point. However, the ACM wizard entails a lengthier configuration. You might be more comfortable running the ACM wizard over the network.

Getting Started with the ACM Wizard (Management Port)

You use the ACM wizard to complete the device configuration.

To get started with the ACM wizard:

1. Run the EasyConfig wizard or QuickStart wizard to assign the management interface an IP address you can reach from your subnet.
2. Connect one end of a CAT-5 cable to the management interface port and the other end to the switch or hub (recommended).
3. Verify that the link LED on the management port is green, indicating an active connection.
4. Return to your desk and open a Web browser.
5. In the browser Address or Location box, enter **https://IP**, where *IP* is the IP address you assigned to the management interface. For example, if you configured the IP address 10.100.200.1, enter **https://10.100.200.1**.



NOTE: ACM access uses SSL, so you must type **https://** and not **http://**.

6. Type the default user name (**root**) and password (**abc123**).
7. Click **ACM** to start the ACM wizard. Complete the wizard steps as described in the online Help.

Installing the Product License Key

IDP 4.1 and later releases require you to install a permanent license key.

To install the permanent license key:

1. Open a Web browser and navigate to the Juniper Networks License Management System Tool (LMS tool):

`https://www.juniper.net/lcrs/license.do`
2. Authenticate with your Juniper Networks customer username and password.
3. Use the LMS tool to generate a new license.

You must provide the device serial number. You can locate the serial number in the following ways:

- In ACM, the serial number is displayed in the lower-left hand corner of the home page.

- From the CLI, run the **scio getsystem** command to display system information, including the serial number.

Save the license as a text file named **lic.txt**.

4. Connect to the IDP command-line interface:
 - Use SSH to connect to the IP address or hostname for the management interface. Log in as the user admin and switch to the user root (**su -u root**).
 - If you prefer, make a connection through the serial port and log in as the user root.

5. Copy the license file to a temporary location on the IDP device.

6. Change directory to the temporary directory:

```
#cd /tmp
```

7. Change permissions on the file to enable read, write, and execute:

```
#chmod 777 lic.txt
```

8. Run the following scio command to add the license key:

```
#scio lic add lic.txt
```

9. Run the following scio command to verify you have successfully added the license key:

```
#scio lic list
```


Chapter 5

Connecting the IDP Traffic Interfaces to Your Network and Verifying Traffic Flow

This chapter includes the following topics:

- Connecting Interfaces to Your Network on page 25
- Verifying Traffic Flow on page 28

Connecting Interfaces to Your Network

This topic provides guidelines for connecting IDP interfaces to your network devices. It includes the following information:

- Deploying Virtual Routers in the Network Path on page 25
- Interface Port Guidelines on page 26
- Cable Guidelines for Copper Ports on page 26
- Connecting and Disconnecting Fiber Cables on page 27

Deploying Virtual Routers in the Network Path

You should choose connections for your IDP device based on your existing network hardware and the networks you want to protect. We recommend you deploy the IDP virtual routers inline, in transparent mode, between gateway firewalls and DMZ or internal networks.

For information about sniffer mode, transparent mode (inline), and mixed mode (one or more virtual routers deployed in each mode), see the *IDP Concepts and Examples Guide*.

Interface Port Guidelines

Table 17 provides guidelines for connecting IDP interfaces to your network.

Table 17: Interface Connection Guidelines

Port	Cable Connection Guidelines
Management Interface	<ol style="list-style-type: none"> 1. Connect one end of a CAT-5 cable into the MGMT port located at the front of the chassis. 2. Connect the other end to a switch or hub (recommended) in your network. <p>Note: NSM must be able to reach the IDP device through this connection.</p>
Traffic Interfaces	<p>Sniffer interfaces - Copper Ports</p> <ol style="list-style-type: none"> 1. Connect one end of a CAT-5 straight-through cable to a traffic interface port located at the front of the chassis. 2. Connect the other end to the Switched Port Analyzer (SPAN) port of a switch or a hub. <hr/> <p>Traffic Interfaces - Copper Ports</p> <p>Adjacent ports belong to exactly one virtual router. For example, interfaces eth2 and eth3 belong to virtual router vr1.</p> <ol style="list-style-type: none"> 1. Connect one end of a CAT-5 cable to the input port of a traffic interface pair (for example, eth2). 2. Connect the other end to an output port of a firewall, switch, or server. 3. Connect one end of a CAT-5 cable to the corresponding output port of a traffic interface pair (for example, eth3). 4. Connect the other end to a corresponding input port of a firewall, switch, or server. <p>For guidelines in choosing a straight-through or crossover cable, see “Cable Guidelines for Copper Ports” on page 26.</p> <hr/> <p>Traffic Interfaces - Fiber Ports</p> <ol style="list-style-type: none"> 1. Connect one end of an LC fiber cable to the input port of a traffic interface pair. 2. Connect the other end to an output port of the switch. 3. Connect one end of an LC fiber cable to the corresponding output port of a traffic interface pair. 4. Connect the other end to a corresponding input port of the switch. <p>See “Connecting and Disconnecting Fiber Cables” on page 27.</p>

Cable Guidelines for Copper Ports

This topic provides guidelines for choosing the correct cables to connect the device to your network devices. It includes the following information:

- Connecting Devices That Support Auto-MDIX on page 27
- Connecting Devices That Do Not Support Auto-MDIX on page 27
- Connecting Devices to Support Internal Bypass on page 27

Connecting Devices That Support Auto-MDIX

If you are connecting devices that support auto-MDIX (medium dependent interface crossover), you can use either straight-through or crossover cables because auto-MDIX negotiates the correct connection.

Connecting Devices That Do Not Support Auto-MDIX

For connections to a firewall or server, use a crossover cable.

For connections to a switch or hub, use a straight-through cable.



Tip: Conventionally, crossover cables have an orange outer jacket. If you are not sure if your Cat 5 cable is a crossover or straight-through cable, lay the two ends side-by-side and observe the order of the wire colors. If the colors are in the same order, it is a straight-through cable; otherwise, it is a crossover cable.

Connecting Devices to Support Internal Bypass

When internal bypass activates, it physically connects the pair of traffic interfaces to each other with a crossover connection.

If the device does not support auto-MDIX, take special care to choose the right cables.

Suppose you plan to place the IDP inline between a firewall and a switch. First, take note of the correct cable choice for a direct connection between the firewall and switch. Would you use a straight-through cable or a cross-over cable?

If the two devices would be connected with a straight-through cable, then use a crossover cable between the firewall and IDP and a straight-through cable between IDP and the switch. When internal bypass activates and crosses-over the connection between the IDP traffic interface pair, the connection between the firewall and the switch will flow as if through a straight-through cable.

If the two devices would be connected with a cross-over cable, then use two straight-through cables. When internal bypass activates, this will have the result of creating one, long cross-over cable connecting the devices.

Connecting and Disconnecting Fiber Cables

The following steps describe how to connect and remove a Gigabit Ethernet cable to and from the transceiver.

To connect a Gigabit Ethernet cable to a transceiver:

1. Hold the cable clip firmly but gently between your thumb and forefinger with your thumb on top of the clip and your finger under the clip. Do not depress the clip ejector on top of the clip.
2. Slide the clip into the transceiver port until it clicks into place. Because the fit is close, you may have to apply some pressure to seat the clip. Apply pressure evenly and gently to avoid clip breakage.

To remove a Gigabit Ethernet cable from a transceiver:

1. Make sure the transceiver ejector under the port is not pressed in; otherwise, if you attempt to remove the cable the transceiver might come out with the cable still attached.
2. Hold the cable clip firmly but gently between your thumb and forefinger with your thumb on top of the clip and your finger under the clip.
3. Use your thumb to gently press the clip ejector on top of the clip. Press down then forward to loosen the clip from the transceiver port.
4. Gently but firmly pull the clip from the transceiver port.

Verifying Traffic Flow

To verify that traffic is flowing through the device:

1. Make sure the device is connected to a live traffic feed.
2. Connect to the IDP command-line interface:
 - Use SSH to connect to the IP address or hostname for the management interface. Log in as **admin** and switch to the user **root** (`su -u root`).
 - If you prefer, make a connection through the serial port and log in as the user **root**.
3. Type **sctop** and press Enter.
4. Type **s** to see status information.
5. Examine the following information on the screen:

Protocol	Packets	Flows	Sessions	Peak	Peak Time
Other	2	0	0	1	05/09/2009 03:08:07
ICMP	3	0	0	0	05/08/2009 18:03:51
UDP	3386	3	1	7	05/08/2009 19:31:01
TCP	151164	12	6	9	05/09/2009 07:01:36

6. Make sure the UDP or TCP values are changing.

Chapter 6

Adding the IDP Device to NSM

This chapter describes how to add the IDP device to Network and Security Manager (NSM). When you complete the procedure to add the IDP device to NSM, NSM updates the IDP device configuration with the default security policy (named Recommended Policy), and the IDP device begins protecting your network.

The procedures in this chapter assume you have installed NSM.

This chapter includes the following topics:

- Reviewing Compatibility with NSM on page 29
- Adding the IDP Device to NSM on page 29
- Checking Device Status on page 33

Reviewing Compatibility with NSM

Review the release notes for information regarding compatibility between your IDP release and NSM release.

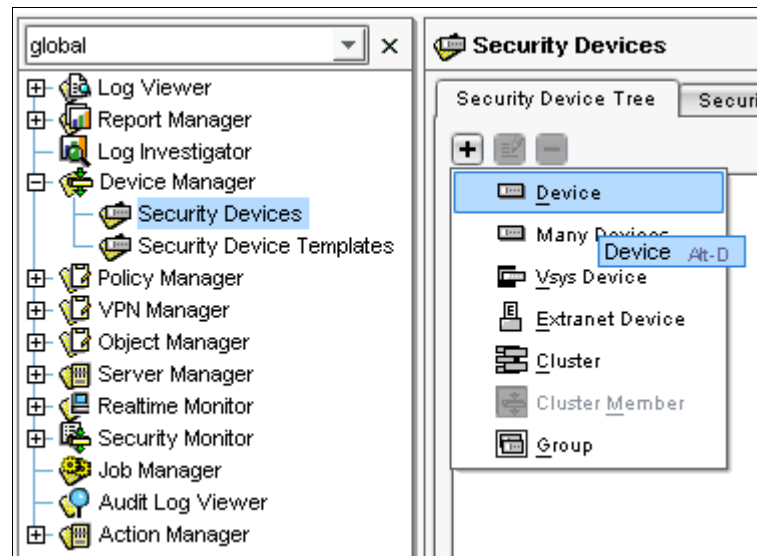
Adding the IDP Device to NSM

This procedure assumes your device is installed, has a static IP address, and is reachable using SSH.

If your device has a dynamic IP address or is not reachable using SSH, see the *Network and Security Manager Administration Guide*.

To import a device with a known IP address:

1. From the domain menu, select the domain in which to import the device.
2. Select **Device Manager** > **Security Devices** from the left navigation pane (Figure 14).

Figure 14: Begin Add Device Procedure

3. On the Security Devices page, click the + button and select **Device** to open the Add Device wizard.
4. Select **Device is Reachable** and click **Next** to display the Specify Connection Settings dialog box (Figure 15).

Figure 15: Add Device Wizard - Connection Settings

 The screenshot shows the 'New Device' dialog box with the 'Specify Connection Settings' tab selected. The form contains the following fields and values:

Field	Value
IP Address	10.100.37.224
Admin User Name	admin
Password	*****
Root User Password for IDP Device	*****
Connect To Device With:	SSH Version 2
Port Number	22

 At the bottom, there is a text instruction: 'Click "Next" to continue.'

5. Enter the following connection information:



NOTE: In NSM, all passwords are case-sensitive.

- a. Enter the IP address you assigned the IDP management interface.

- b. Enter **admin** in the Admin User Name box.
- c. Enter the password for the user admin. The default is abc123.
- d. Enter the password for the user root. The default is abc123.
- e. Select **SSH Version 2** as the connection method. Leave the port number as 22.
- f. Click **Next** to open the Verify Device Authenticity dialog box (Figure 16). After a moment, the wizard displays the SSH key fingerprint information.

Figure 16: Add Device Wizard - Verification Settings



6. Log into the IDP command-line interface and verify the SSH key fingerprint. Comparing the SSH key fingerprint information enables you to detect man-in-the-middle attacks:
 - a. Connect to the IDP command-line interface:
 - Use SSH to connect to the IP address or hostname for the management interface. Log in as admin and switch to the user root (**su -u root**).
 - If you prefer, make a connection through the serial port and log in as the user root.
 - b. Type **cd /etc/ssh** and press Enter.
 - c. Type **ssh-keygen -l -f ssh_host_dsa_key** and press Enter.

The command generates output similar to the following:

```
1024 f4:91:d0:04:b7:61:00:77:45:c3:cc:bd:af:b3:5b:a2 ssh_host_dsa_key.pub
```

7. After you have verified the key, click **Next** to display device information retrievable by NSM (see Figure 17). This takes a moment.

Figure 17: Add Device Wizard - Retrieved Settings

New Device	
Auto Detecting Device	
IP Address	10.100.37.224
Device Type	NS-IDP
Managed OS Version	IDP 5.x
Running OS Version	IDP 5.xxx
Support Level	Full Support
Serial Number	0148032005000004
IDP Mode	Transparent
Device autodetected successfully. Click Next To Proceed...	

8. Verify that the device type, OS version, device serial number, and device mode are correct.
9. Click **Next** to add the device to NSM as a managed device. (See Figure 18.)

Figure 18: Add Device Wizard - Adding the Device

New Device	
Adding device	
Device has been added to NSM and is ready for Import. Click 'Next' to Import Device Config	

10. Click **Next** to have NSM import settings already present on the device. (See Figure 19.)

Figure 19: Add Device Wizard - Importing the Device

New Device	
Importing Device	
Device Imported Successfully to NSM. Click 'Finish' to Update the Device with Recommended Policy.	

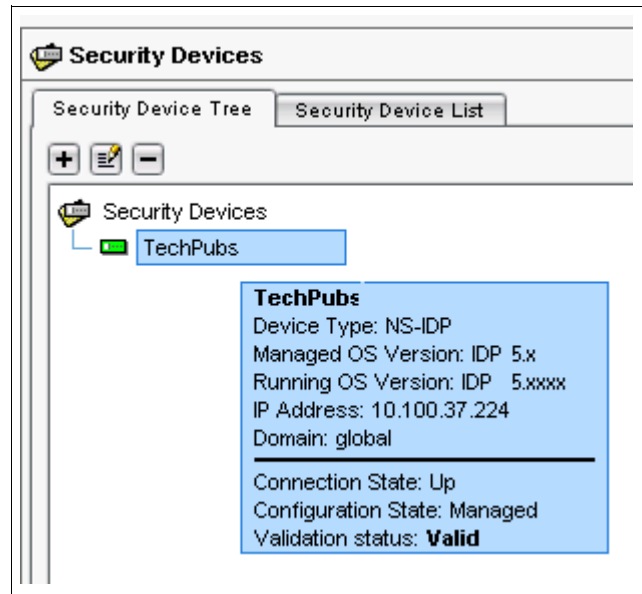
11. Click **Finish** to update the device with the default policy (named Recommended Policy).

The Job Information dialog box shows the status of the Update Device job.

Checking Device Status

When the update device job finishes, move the mouse pointer over the device in Device Manager to check the device status. The configuration state **Managed** indicates that the device is connected and that the management system has successfully imported the device configuration (Figure 20).

Figure 20: Viewing Device Status



NSM is now managing your device.

For more information about using NSM to manage IDP devices, see the *Network and Security Manager Administration Guide*.

Chapter 7

Updating Software

This chapter provides procedures for performing software upgrades—either from NSM or locally on the device. It includes the following topics:

- Upgrade Paths on page 35
- Updating IDP Software (NSM Procedure) on page 35
- Upgrading IDP Software (CLI Procedure) on page 37

Upgrade Paths

Read the release notes for a list of supported upgrade paths.

Updating IDP Software (NSM Procedure)

You can use NSM to upgrade IDP software on all of your devices.

Follow these basic steps:

1. Load a new software image to NSM. See “Loading a Software Image in NSM” on page 35.
2. Use NSM to install the new image on devices. See “Pushing Software to IDP Devices” on page 36.

Loading a Software Image in NSM

To load a new software image in NSM:

1. Download the software image to the NSM GUI server.
 - a. Go to <https://www.juniper.net/customers/csc/software/> and log in with your customer user name and password.
 - b. Navigate to **IDP > ScreenOS Software Downloads (including NSM/Global Pro, STRM, IDP and NetScreen-Remote)**.
 - c. In the row for IDP, click **5.0**.

- d. Save the `sensor_version.sh` file to the NSM GUI server (where *version* is the number that identifies the software release version).
2. In NSM, select **Device Manager > Security Devices** from the left navigation pane.
3. From the menu bar, select **Tools > Software Manager** to display the Software Manager dialog box.
4. Click the **+** button to open the Open dialog box.
5. Select the **sensor_version.sh** file you downloaded and click **Open**. The image file appears in the Software Manager dialog box, displaying the image name, version, and applicable devices.
6. Click **OK**.

Pushing Software to IDP Devices

After you have made the software available to NSM, you can use NSM to upgrade the device.

To upgrade the device using NSM:

1. From the menu bar, select **Devices > Software > Install Device Software** and complete the wizard steps.
2. Click **Finish** to display upgrade status in the Job Information dialog box.
3. When the upgrade finishes, click **Close** to exit the Job Information dialog box.

Next Steps

1. In the NSM Device Manager, right-click the IDP device and select **Import Device**.
2. Check to see if J-Security Center has released an update for the detector engine or attack database:

From the NSM main menu, select **Tools > View/Update NSM attack database** and complete the wizard steps.

3. Push the updated IDP detector engine to IDP devices:

From the NSM main menu, select **Devices > IDP Detector Engine > Load IDP Detector Engine for ScreenOS** and complete the wizard steps.

4. Push a security policy update job to update attack objects in use in your security policy. In NSM, select **Devices > Configuration > Update Device Config** and complete the wizard steps.



NOTE: We recommend you schedule automatic updates for the NSM attack database. For details, see the *Network and Security Manager Administration Guide*.

Upgrading IDP Software (CLI Procedure)

To install the new software from the command line:

1. Download the software image:
 - a. Go to <https://www.juniper.net/customers/csc/software/> and log in with your customer user name and password.
 - b. Navigate to **IDP > ScreenOS Software Downloads (including NSM/Global Pro, STRM, IDP and NetScreen-Remote)**.
 - c. In the row for IDP, click **5.0**.
 - d. Save the `sensor_version.sh` file (where *version* is the number that identifies the software release version).
2. Connect to the IDP command-line interface:
 - Use SSH to connect to the IP address or host name for the management interface. Log in as admin and switch to the user root (`su -u root`).
 - If you prefer, make a connection through the serial port and log in as the user root.



NOTE: To make an SSH connection, you must have enabled SSH for the management port (eth0). For details, see the ACM online Help.

3. Use SCP or FTP to copy the software image to the IDP device. IDP does not run an FTP server, so you have to initiate the FTP session from the IDP device.
4. Run the upgrade script by typing `sh sensor_version.sh`, where *version* is the number that identifies the software release version. Press Enter.
5. When the script has finished, type **reboot** and press Enter.

In the NSM Device Manager, right-click the device, select **Adjust OS Version**, and complete the wizard steps.

Next Steps

Next Steps

1. In the NSM Device Manager, right-click the IDP device and select **Import Device**.
2. Check to see if J-Security Center has released an update for the detector engine or attack database:

From the NSM main menu, select **Tools > View/Update NSM attack database** and complete the wizard steps.

3. Push the updated IDP detector engine to IDP devices:

From the NSM main menu, select **Devices > IDP Detector Engine > Load IDP Detector Engine for ScreenOS** and complete the wizard steps.

4. Push a security policy update job to update attack objects in use in your security policy. In NSM, select **Devices > Configuration > Update Device Config** and complete the wizard steps.



NOTE: We recommend you schedule automatic updates for the NSM attack database. For details, see the *Network and Security Manager Administration Guide*.

Chapter 8

Reimaging the IDP Appliance

This chapter includes the following topic:

- Reimaging the IDP Appliance on page 39

Reimaging the IDP Appliance

The appliance comes with software pre-installed. If needed, you can reinstall the factory image. This process is known as *reimaging* the appliance:

To reimage the appliance:

1. Connect a PC to the serial console port of the device using the null-modem serial cable provided with the appliance.
2. Insert the CD that came with the appliance into the CD-ROM drive at the back of the device and reboot the appliance. If you have misplaced the CD that came with the appliance, contact Juniper Networks Technical Assistance Center (JTAC).

The appliance boots from the CD and runs the reimaging process. Follow any prompts on the serial console.

3. When the reimaging process has completed, remove the CD and reboot.
4. Configure the appliance according to the instructions in “If your model has redundant power supplies, repeat the previous steps to connect the second power supply.” on page 18.
5. Relicense the appliance as described in “Installing the Product License Key” on page 23.

Chapter 9

Installing Field Replaceable Units

This chapter describes how to install a field replaceable unit (FRU). It includes the following topics:

- Replacing a Power Supply on page 41
- Replacing a Hard Drive on page 43

Replacing a Power Supply

The IDP 200 has one power supply and an empty bay for a second power supply. The IDP 600 and 1100 have two power supplies.

If a device has two power supplies, one of the power supplies may be hot swapped while the device is running.

For information on obtaining spares, contact your Juniper Networks sales representative.

To remove a power supply or blank:

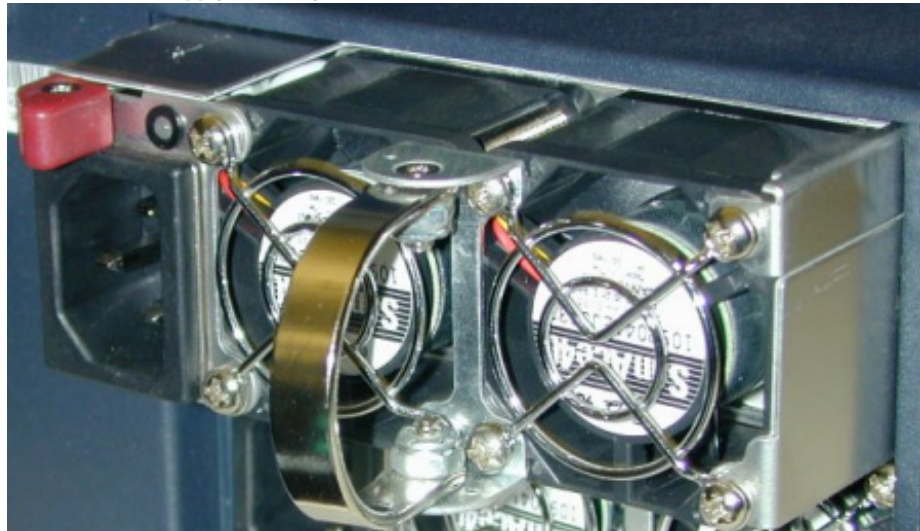
1. Go to the back of the device.
2. Identify the power supply or blank you want to remove. See Figure 21.

Figure 21: Power Supply Handles in Open and Closed Positions



3. On the power supply or blank you want to remove, rotate the curved handle to the open (extended) position.
4. Grasp the extended handle with one hand.
5. In the upper left corner of the power supply or blank is a red lever. Push it to the right to unlatch it. See Figure 22.

Figure 22: Power Supply Partially Removed



6. With the red lever pushed to the right, pull firmly on the extended handle until the power supply or blank begins to slide out.

7. Let go of the red handle and use both hands to slide the power supply or blank the rest of the way out.

To install a power supply:

1. Take the new power supply to the back of the device.
2. Extend the curved handle so you have a good place to grab.
3. Hold the power supply in both hands. With one hand hold the extended handle. With the other hand, hold the power supply from underneath.
4. Line the power supply up with the empty bay. The red handle should be in the upper left corner above the power plug port.
5. Slide the power supply into the bay.
6. Push firmly until you see and hear the latch (the red lever) snap into place. Both power supplies should now be even with each other.

If the other power supply is on and powering the device, the device emits a high-pitched whine and the PS FAIL light on the front of the appliance turns on.

7. Connect a power cord to the new power supply.
8. Attach the other end of the power cord to the plug strip.

The power supply LED glows amber to indicate that the power supply is receiving power. It glows green to indicate that it is receiving power and is giving power to the appliance (only occurs if the appliance is on). The high-pitched whine stops and the PS FAIL light on the front of the appliance turns off.

Replacing a Hard Drive

The IDP 600 and 1100 models come with two SCSI RAID 1 mirrored hard drives. Both drives are hot-swappable on failure. If one fails it may be replaced without interrupting the function of the appliance.

For information on obtaining spares, contact your Juniper Networks sales representative.



CAUTION: The RAID array is designed to provide fault tolerant redundancy in the device. Do not remove a drive unless it has failed. The red failure LED turns on if a drive has failed. Only remove a drive if its red LED is on.



CAUTION: When one drive is replaced, it takes some time for all the data from the second drive to be mirrored over to the new drive. Do not remove either drive during a rebuild.

To remove a hard drive:

1. Go to the back of the device.
2. Identify the hard drive you want to remove.

The left-most LED on a drive is red when the drive has failed.

3. Locate the handle release latch on the right side of the drive, above the LEDs. See Figure 23.

Figure 23: Hard Drive Latch in Open Position, Handle Released



4. Press the latch down to release the handle. See Figure 24.

Figure 24: Hard Drive Handle Down



5. Pull the handle down to the horizontal position. This action unlatches the drive and moves it part way out of the bay. See Figure 25.

Figure 25: Drive Partially Removed



6. Pull the handle to slide the drive out of the bay. When the drive is partially visible, use a second hand to hold the drive from underneath.
7. Using both hands, remove the drive completely from the bay.

To install a hard drive:

1. Unclip the latch on the right side of the handle.
2. Lower the handle to the fully extended, horizontal position.
3. Grasp the handle with one hand. Support the drive from underneath with the other.
4. Begin to slide the drive into the bay. See Figure 26.

Figure 26: Drive Partially Inserted

5. Gently slide the drive the rest of the way into the bay.
6. When the drive stops moving easily, raise the handle of the drive. See Figure 27. This action engages a lever that pulls the drive the rest of the way into the bay.

Figure 27: Hard Drive Latch in Closed Position

7. Press the drive handle up until the latch clicks into place.

After a few moments, the warning sound will cease; the red failure light on the new drive will begin to flash, indicating that the RAID is being rebuilt; and the hard drive activity light on both drives will flash, indicating activity on both drives.

When the red failure light stops flashing, the RAID is rebuilt. Rebuilding the RAID may take some time (30 minutes or more.)

Leave both drives in place until the RAID array is rebuilt. Removing either drive while the RAID array is being rebuilt can damage the system.

Appendix A

Specifications

This appendix is a reference of physical, power, and environmental specifications for IDP models. It also states compliance with standards for safety and electromagnetic interference and immunity. This appendix includes the following topics:

- IDP200 Technical Specifications on page 49
- IDP600 Technical Specifications on page 51
- IDP1100 Technical Specifications on page 52
- Safety Compliance on page 54
- EMI Compliance on page 54
- Immunity on page 54

IDP200 Technical Specifications

Tables 18 through 21 give the physical, AC power, power cord, and environmental specifications.

Table 18: IDP200 Physical Specifications

Specification	Value
Form Factor	2 RU
Height	3.4 in. (8.64 cm)
Width	17 in. (43.2 cm)
Depth	20.5 in. (51.18 cm)
Weight	29.5 lb (13.38 kg)

Table 19: IDP200 AC Power Specifications

Specification	Nominal Value	Acceptable Range
AC input voltage	110/220 VAC, single phase	90 to 255 VAC

Table 19: IDP200 AC Power Specifications (continued)

Specification	Nominal Value	Acceptable Range
AC input line frequency	50/60 Hz	47 to 63 Hz
AC input current	4A @ 110 VAC 2A @ 220 VAC	

Table 20: IDP200 Power Cord Specifications

Country	Specifications
United States and Canada	<ul style="list-style-type: none"> ■ UL-approved and CSA-certified ■ Flexible cord minimum spec: No. 18 (1.5 mm²), Type SVT or SJT, 3-conductor ■ Current capacity of 10A minimum ■ Earth-grounding attachment plug with NEMA 5-15P (10A, 125V) configuration

Table 21: IDP200 Environmental Specifications

Specification	Value
Operating temperature	50° to 95° F (10° to 35° C)
Storage temperature	-40° to 158° F (-40° to 70° C)
Relative humidity (operating)	8 % to 90 % noncondensing
Relative humidity (storage)	5 % to 95 % noncondensing
Altitude (operating)	-50 to 10,000 ft (-15.24 m to 3,048 m)
Altitude (storage)	-50 to 35,000 ft (-15.24m to 10,668 m)

Heat dissipation rates depend on the traffic rate and the number and type of features you have enabled. Table 22 provides guidelines.

Table 22: IDP200 Heat Dissipation Guidelines

Specification	Watts	BTU/hour
Minimum	156	532.29
Load	256	873.51
Maximum	282	962.22

IDP600 Technical Specifications

Tables 23 through 26 give the physical, AC power, power cord, and environmental specifications.

Table 23: IDP600 Physical Specifications

Specification	Value
Form Factor	2 RU
Height	3.4 in. (8.64 cm)
Width	17 in. (43.2 cm)
Depth	20.5 in. (51.18 cm)
Weight	33.5 lb (15.20 kg)

Table 24: IDP600 AC Power Specifications

Specification	Nominal Value	Acceptable Range
AC input voltage	110/220 VAC, single phase	90 to 255 VAC
AC input line frequency	50/60 Hz	47 to 63 Hz
AC input current	4A @ 110 VAC 2A @ 220 VAC	

Table 25: IDP600 Power Cord Specifications

Country	Specifications
United States and Canada	<ul style="list-style-type: none">■ UL-approved and CSA-certified■ Flexible cord minimum spec: No. 18 (1.5 mm²), Type SVT or SJT, 3-conductor■ Current capacity of 10A minimum■ Earth-grounding attachment plug with NEMA 5-15P (10A, 125V) configuration

Table 26: IDP600 Environmental Specifications

Specification	Value
Operating temperature	50° to 95° F (10° to 35° C)
Storage temperature	-40° to 158° F (-40° to 70° C)
Relative humidity (operating)	8 % to 90 % noncondensing
Relative humidity (storage)	5 % to 95 % noncondensing
Altitude (operating)	-50 to 10,000 ft (-15.24 m to 3,048 m)
Altitude (storage)	-50 to 35,000 ft (-15.24m to 10,668 m)

Heat dissipation rates depend on the traffic rate and the number and type of features you have enabled. Tables 27 and 28 provide guidelines.

Table 27: IDP600C Heat Dissipation Guidelines

Specification	Watts	BTU/hour
Minimum	210	716.55
Load	306	1044.12
Maximum	337	1149.89

Table 28: IDP600F Heat Dissipation Guidelines

Specification	Watts	BTU/hour
Minimum	210	716.55
Load	283	965.64
Maximum	311	1061.18

IDP1100 Technical Specifications

Tables 29 through 32 give the physical, AC power, power cord, and environmental specifications for the IDP1100 appliance.

Table 29: IDP1100 Physical Specifications

Specification	Value
Form Factor	2 RU
Height	3.4 in. (8.64 cm)
Width	17 in. (43.2 cm)
Depth	20.5 in. (51.18 cm)
Weight	36.5 lb (16.56 kg)

Table 30: IDP1100 AC Power Specifications

Specification	Nominal Value	Acceptable Range
AC input voltage	110/220 VAC, single phase	90 to 255 VAC
AC input line frequency	50/60 Hz	47 to 63 Hz
AC input current	4A @ 110 VAC 2A @ 220 VAC	

Table 31: IDP1100 Power Cord Specifications

Country	Specifications
United States and Canada	<ul style="list-style-type: none"> ■ UL-approved and CSA-certified ■ Flexible cord minimum spec: No. 18 (1.5 mm²), Type SVT or SJT, 3-conductor ■ Current capacity of 10A minimum ■ Earth-grounding attachment plug with NEMA 5-15P (10A, 125V) configuration

Table 32: IDP1100 Environmental Specifications

Specification	Value
Operating temperature	50° to 95° F (10° to 35° C)
Storage temperature	-40° to 158° F (-40° to 70° C)
Relative humidity (operating)	8 % to 90 % noncondensing
Relative humidity (storage)	5 % to 95 % noncondensing
Altitude (operating)	-50 to 10,000 ft (-15.24 m to 3,048 m)
Altitude (storage)	-50 to 35,000 ft (-15.24m to 10,668 m)

Heat dissipation rates depend on the traffic rate and the number and type of features you have enabled. Tables 33 and 34 provide guidelines.

Table 33: IDP1100C Heat Dissipation Guidelines

Specification	Watts	BTU/hour
Minimum	260	887.16
Load	450	1535.46
Maximum	495	1689.01

Table 34: IDP1100C Heat Dissipation Guidelines

Specification	Watts	BTU/hour
Minimum	260	887.16
Load	430	1467.22
Maximum	473	1613.94

Safety Compliance

- UL 60950, Third Edition — Safety of Information Technology Equipment
- CSA C2.22 No. 60950, Third Edition — Safety of Information Technology Equipment
- EN 60950, 2000 — Safety of Information Technology Equipment, including Electrical Business Equipment
- IEC 60950, Third Edition — Safety of Information Technology Equipment, including Electrical Business Equipment

EMI Compliance

- EN 55022, 1998 Class A
- EN 61000-3-2
- FCC Part 15 Class A
- Industry Canada ICES-003 Class A
- VCCI Class A

Immunity

- EN 55024, 1998

Appendix B

Common Criteria EAL2 Compliance

This appendix provides guidelines you must observe to deploy and use the IDP device in compliance with the Common Criteria EAL2.

In addition, you must observe compliance guidelines for Network and Security Manager (NSM), listed in the *Network and Security Manager Administration Guide*.

This appendix contains the following topics:

- Guidance for Intended Usage on page 55
- Guidance for Personnel on page 55
- Guidance for Physical Protection on page 56

Guidance for Intended Usage

- The IDP device must be connected to the network from which IT systems are to be monitored to collect data or to prevent certain data from passing to or from IT systems.
- The IDP device must be appropriately scalable to the IT system that it monitors.
- The IDP device must be managed in a manner that allows it to address changes in the IT system that it monitors.
- The IDP device, the NSM device server and GUI server, and the NSM UI must be installed on dedicated systems. These dedicated systems must not contain user processes that are not required to operate the IDP system.

Guidance for Personnel

- There must be one or more authorized individuals assigned to manage the IDP device, NSM, and the security of the information that they contain.
- The authorized administrators must not be careless, willfully negligent, or hostile and must follow and abide by the instructions provided by the IDP device, NSM, and UI documentation.
- The IDP device and NSM must be accessed only by authorized users.

Guidance for Physical Protection

The processing resources of the IDP device, the NSM server, and the NSM UI must be located within facilities with controlled access that prevents unauthorized physical access.

Index

Numerics

1998 Class A compliance 54

A

ACM 10, 19, 23
Administration Guide xv
audience for documentation xiii
auto-MDIX 26

B

BTU/hour
 IDP 1100 53
 IDP 200 50
 IDP 600 52
bypassStatus utility 10

C

CD-ROM drive 8
central management software 10
classes, Juniper IDP xvi
Common Criteria EAL2 compliance 55
compliance
 Common Criteria EAL2 55
 EMI standards 54
 immunity standards 54
Concepts & Examples Guide xv
configuring the device 19–23
connecting power 17
console serial port 4
copper ports
 cable guidelines 26
CSA C2.22 No. 60950 compliance 54
customer support center xvi, 39

D

DB-9 serial port 4
DNS, setting 20
documentation
 downloads xvi
 list of xiv
downloads xvi

E

EasyConfig 9, 19, 20
education services xvi
EMI compliance 54
EMI compliance specifications 54
EN 1998 compliance 54

EN 2000 compliance 54
EN 55022 compliance 54
EN 55024 compliance 54
EN 60950 compliance 54
EN 61000-3-2 compliance 54
environmental specifications 49–54
equipment rack 15

F

FCC Part 15 Class A compliance 54
fiber ports
 cables 27
field replaceable units 41–47
forum, Juniper Networks Community Forum xvi
FRU 41–47

H

HA port
 LEDs 5
 overview 5
hard drives 7
 replacing 43
heat dissipation
 IDP 1100 53
 IDP 200 50
 IDP 600 52
high availability options 20
hot-swappable hard drives 7

I

ICES-003 Class A compliance 54
IDP 1100
 appliance LEDs 3
 hard drives 7
 heat dissipation 53
 power supplies 8
 replacing hard drives 43
 replacing power supplies 41
 technical specifications 52
IDP 1100C 3
IDP 1100F 3
IDP 200 2
 appliance LEDs 3
 hard drives 7
 heat dissipation 50
 power supply 8
 replacing power supplies 41
 technical specifications 49
IDP 200/600/1100 Installation Guide xv

IDP 50	
rack mounting kit	15
IDP 600	
appliance LEDs	3
hard drives	7
heat dissipation	52
power supplies	8
replacing hard drives	43
replacing power supplies	41
technical specifications	51
IDP 600C	2
IDP 600F	2
IDP 75/250/800/8200 Installation Guide	xv
IDP ACM Online Help	xv
IDP documentation set	xiv
IDP Reporter User's Guide	xv
idp.sh utility	10
IEC 60950 safety compliance	54
immunity standards	54
Industry Canada ICES-003 Class A compliance	54
Installation Guide	xv
installing the device	15
interoperation, password for	20
Intrusion Detection and Prevention Administration Guide	xv
Intrusion Detection and Prevention Concepts & Examples Guide	xv
J	
JTAC	xvi, 39
Juniper Networks Safety Guide	xv
Juniper Secure Access interoperation	20
Juniper Unified Access Control interoperation	20
K	
knowledge base	xvi
L	
Layer 2 bypass setting	20
LEDs	
HA port	5
hard drive	8
HD	3
IDP 1100C	3
IDP 1100F	3
IDP 200	2
IDP 600C	2
IDP 600F	2
management port	4
overheat	3
power	3
power supply	8
traffic interface	6
M	
management console, connecting to	19
management interface, choosing cable for	26
management port	
LEDs	4
overview	4
MDIX	26
mounting the device	15
N	
Network and Security Manager Administration Guide	xv
Network and Security Manager Configuring Intrusion Detection and Prevention Devices Guide	xv
NSM	
adding IDP to	29
documentation	xv
overview	10
specifying connection information for	20
NTP, setting	20
O	
on-box management software	9
one time password	20
online help	xv
P	
ports	
copper	26
fiber	26
IDP 1100C	3
IDP 1100F	3
IDP 200	2
IDP 600C	2
IDP 600F	2
power specifications	49–54
power supplies	8
connecting	17
LEDs	8
replacing	41
Q	
QuickStart	9, 19, 22, 23
R	
rack-mounting kit	15
RADIUS, configuring	20
re-imaging the appliance	39
re-imaging the device	37
release Notes	xiv, xv
replacing	
hard drives	43
power supplies	41
S	
safety compliance standards	54
safety guidelines	14
scio utility	10
SCSI drives	7
sctop utility	10, 28
security guidelines	14
sensor_version.sh	37
serial port console	
connecting to	19
description of	4

sniffer mode	
setting	20
software	
on-box	9
upgrade	35-??
specifications	49-54
EMI compliance	54
IDP 1100	52
IDP 200	49
IDP 600	51
immunity	54
safety compliance	54
SSH-access, configuring	20
standards	
Common Criteria EAL2	55
EMI compliance	54
safety compliance	54

T

technical bulletins	xvi
technical specifications	49-54
technical support	xvi, 39
traffic flow, verifying	28
traffic interfaces	
choosing cables for	26
copper ports	26
fiber ports	26
transparent mode	
setting	20

U

UL 60950 compliance	54
upgrading software	35-??

V

VCCI Class A compliance	54
verifying traffic flow	28

