



---

# IDP Series Intrusion Detection and Prevention Appliances

## IDP75 Installation Guide

Release

5.x



Published: 2012-08-16

Part Number: 530-029728-01, Revision 03

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

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

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

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

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

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

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

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

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

*IDP Series Intrusion Detection and Prevention Appliances IDP75 Installation Guide*

Copyright © 2012, Juniper Networks, Inc.

All rights reserved.

Revision History

April 2011—03

The information in this document is current as of the date on the title page.

## END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

	<b>Preface</b> .....	<b>v</b>
	Objectives .....	v
	Audience .....	v
	Documentation Conventions .....	v
	Related Documentation .....	vii
	Requesting Technical Support .....	viii
	Self-Help Online Tools and Resources .....	viii
	Opening a Case with JTAC .....	ix
<b>Part 1</b>	<b>Hardware and Software Overview</b>	
<b>Chapter 1</b>	<b>Hardware Overview</b> .....	<b>3</b>
	IDP75 Overview .....	3
	Power Supply .....	4
	Hard Drive .....	4
	Fans .....	4
	System Status LEDs .....	4
	USB Port .....	5
	Serial Console Port .....	5
	Management Interface Port .....	5
	Traffic Interface Ports .....	6
	Copper Ports .....	6
	Traffic Interface Features .....	7
	Deployment Mode .....	7
	Layer 2 Bypass .....	8
	Internal Bypass .....	8
	External Bypass .....	10
	NICs Off .....	10
	Peer Port Modulation .....	11
<b>Chapter 2</b>	<b>Software Overview</b> .....	<b>13</b>
	On-Box Software Overview .....	13
	Centralized Management with NSM Overview .....	14
	J-Security Center Updates Overview .....	15
<b>Part 2</b>	<b>Performing the Installation</b>	
<b>Chapter 3</b>	<b>Installation Overview</b> .....	<b>19</b>
	Before You Begin .....	19
	Basic Steps .....	20

<b>Chapter 4</b>	<b>Installing the Appliance to Your Equipment Rack and Connecting Power</b> . . . . .	<b>21</b>
	Rack Mounting Kits and Required Tools . . . . .	21
	Mounting to Midmount Brackets . . . . .	22
	Mounting to Rack Rails . . . . .	23
	Connecting Power . . . . .	23
<b>Chapter 5</b>	<b>Performing the Initial Network Configuration and Licensing Tasks</b> . . . . .	<b>25</b>
	Performing the Initial Configuration . . . . .	25
	Getting Started with the EasyConfig Wizard (Serial Console Port) . . . . .	27
	Getting Started with the QuickStart Wizard (Management Port) . . . . .	28
	Getting Started with the ACM Wizard (Management Port) . . . . .	29
	Installing the Product License Key . . . . .	29
<b>Chapter 6</b>	<b>Connecting the IDP Series Traffic Interfaces to Your Network and Verifying Traffic Flow</b> . . . . .	<b>31</b>
	Guidelines for Connecting IDP Series Interfaces to Your Network Devices . . . . .	31
	Choosing Cables for Traffic Interfaces (Copper Ports) . . . . .	32
	Connecting Devices That Support Auto-MDIX . . . . .	33
	Connecting Devices That Do Not Support Auto-MDIX . . . . .	33
	Connecting Devices to Support Internal Bypass . . . . .	33
	Connecting and Disconnecting Fiber Cables . . . . .	33
	Verifying Traffic Flow . . . . .	34
<b>Part 3</b>	<b>Adding the IDP Series Device to NSM</b>	
<b>Chapter 7</b>	<b>Adding the IDP Series Device to NSM</b> . . . . .	<b>39</b>
	Reviewing Compatibility with NSM . . . . .	39
	Adding a Reachable IDP Series Device to NSM . . . . .	39
<b>Part 4</b>	<b>Upgrading Software</b>	
<b>Chapter 8</b>	<b>Upgrading Software</b> . . . . .	<b>47</b>
	Updating Software (NSM Procedure) . . . . .	47
	Upgrading Software (CLI Procedure) . . . . .	49
<b>Chapter 9</b>	<b>Reimaging the Appliance</b> . . . . .	<b>51</b>
	Reimaging and Relicensing an Appliance . . . . .	51
<b>Part 5</b>	<b>Technical Specifications and Compliance Statements</b>	
<b>Chapter 10</b>	<b>Technical Specifications</b> . . . . .	<b>55</b>
	IDP75 Technical Specifications . . . . .	55
<b>Chapter 11</b>	<b>Compliance Statements</b> . . . . .	<b>57</b>
	Standards Compliance . . . . .	57
<b>Part 6</b>	<b>Index</b>	
	Index . . . . .	61

# Preface

This preface includes the following topics:

- [Objectives on page v](#)
- [Audience on page v](#)
- [Documentation Conventions on page v](#)
- [Related Documentation on page vii](#)
- [Requesting Technical Support on page viii](#)

## 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.

## Documentation Conventions

---

This section provides all the documentation conventions that are followed in this guide. [Table 1 on page v](#) defines notice icons used in this guide.

**Table 1: Notice Icons**





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

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

Table 2: Text Conventions

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

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

Table 3: Syntax Conventions

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

## Related Documentation

Table 4 on page vii lists related IDP Series documentation.

**Table 4: Related IDP Series Documentation**

Document	Description
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.
ACM Online Help	Available through the Appliance Configuration Manager (ACM). The context-sensitive online help describes how to use the QuickStart and ACM Wizard pages to configure network settings, network interfaces, and NIC features.
<ul style="list-style-type: none"> <li>• <i>IDP Series Installation Guide: IDP200, IDP600, IDP1100</i></li> <li>• <i>IDP75 Installation Guide</i></li> <li>• <i>IDP250 Installation Guide</i></li> <li>• <i>IDP800 Installation Guide</i></li> <li>• <i>IDP8200 Installation Guide</i></li> </ul>	Provides instructions for installing, configuring, updating, and servicing the IDP Series appliances.
<i>IDP Concepts and Examples Guide</i>	Explains IDP features and provides examples of how to use the system.
<i>IDP Administration Guide</i>	Provides procedures for implementing IDP features, monitoring performance, and monitoring security events.
<i>IDP Custom Attack Objects Reference and Examples Guide</i>	Provides in-depth examples and reference information for creating custom attack objects.
<i>IDP Reporter User's Guide</i>	Describes how to use IDP Reporter to view and generate security reports and application usage reports.

Table 4 on page vii lists related NSM documentation.

**Table 5: Related NSM Documentation**

Document	Description
Network and Security Manager release notes	Provides information about new features, changed features, fixed problems, and known issues with the NSM release.
<i>Network and Security Manager Installation Guide</i>	Describes how to install the NSM management system on a single server or on separate servers. It also includes information on how to install and run the NSM user interface. This guide is intended for IT administrators responsible for the installation and/or upgrade to NSM.

Table 5: Related NSM Documentation (*continued*)

Document	Description
<i>Network and Security Manager Configuring Intrusion Detection and Prevention Devices Guide</i>	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.
<i>Network and Security Manager Administration Guide</i>	<p>Describes how to use and configure key management features in the NSM. It provides conceptual information, suggested workflows, and examples where applicable. This guide is best used in conjunction with the NSM Online Help, which provides step-by-step instructions for performing management tasks in the NSM UI.</p> <p>This guide is intended for application administrators or those individuals responsible for owning the server and security infrastructure and configuring the product for multi-user systems. It is also intended for device configuration administrators, firewall and VPN administrators, and network security operation center administrators.</p>
Network and Security Manager Online Help	Provides task-oriented procedures describing how to perform basic tasks in the NSM user interface. It also includes a brief overview of the NSM system and a description of the GUI elements.

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf> .
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/> .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>



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

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

## Opening a Case with JTAC

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

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

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



## PART 1

# Hardware and Software Overview

- [Hardware Overview on page 3](#)
- [Software Overview on page 13](#)



## CHAPTER 1

# Hardware Overview

This chapter includes the following topics:

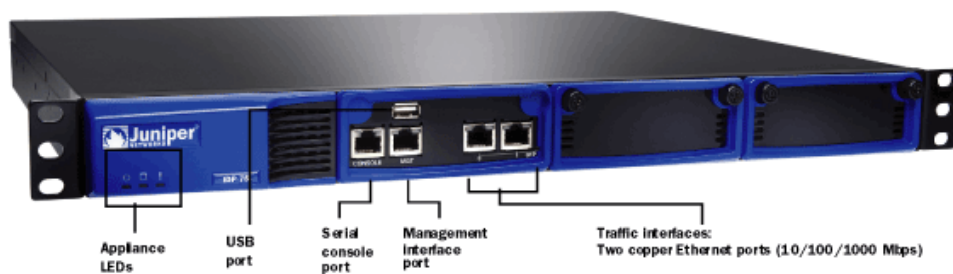
- [IDP75 Overview on page 3](#)
- [Power Supply on page 4](#)
- [Hard Drive on page 4](#)
- [Fans on page 4](#)
- [System Status LEDs on page 4](#)
- [USB Port on page 5](#)
- [Serial Console Port on page 5](#)
- [Management Interface Port on page 5](#)
- [Traffic Interface Ports on page 6](#)

## IDP75 Overview

---

The IDP75 appliance is optimal for small networks or low-speed network segments. [Figure 1 on page 3](#) shows the location of appliance LEDs and ports.

Figure 1: IDP75 Front Panel



### Related Documentation

- [System Status LEDs on page 4](#)
- [USB Port on page 5](#)
- [Serial Console Port on page 5](#)
- [Management Interface Port on page 5](#)
- [Traffic Interface Ports](#)

- [IDP75 Technical Specifications on page 55](#)

## Power Supply

The appliance has one fixed power supply. It is not a field replaceable unit (FRU).

You can order a replacement power cord through your Juniper Networks sales contact. The part number for the power cord is CBL-JX-PWR-*Country* (varies by country).

## Hard Drive

The appliance has one 80 GB hard drive. It is not a field replaceable unit (FRU).

## Fans




When the system is cool, appliance 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 appliance fault LED blinks and the remaining fan or fans run at full speed until the failed fan is replaced.

The fans for this model are not field replaceable units (FRUs).

## System Status LEDs

[Table 6 on page 4](#) describes system status LED states.

**Table 6: System Status LED States**

LED	Status	Description
	Solid green	System is powered on.
	Off	System is powered off.
	Flashing amber	Hard disk is active.
	Off	Hard drive has no activity.
	Slowly blinking red	Power failure.
	Quickly blinking red	Fan failure.
	Solid red	Overheating.
	Off	Heat and power are normal.

## USB Port

The appliance has a USB port you can use to reimage the appliance, if necessary. The part number is IDP-FLASH (IDP75, IDP250, IDP800) or IDP-FLASH-8200 (IDP8200).

## Serial Console Port

The console serial port provides access, using an RJ-45 connector, to the command-line interface (CLI).



**NOTE:** Although both the console serial port and the management port use RJ-45 connectors, do not plug the network cable into the console serial port.

## Management Interface Port

The management interface port is a 10/100/1000 Mbps Ethernet port. In the configuration and logs, the port is **eth0**. Use this 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 2 on page 5 shows the management interface port LEDs.

Figure 2: Management Interface Port LEDs



Table 7 on page 5 describes the management interface port LED states.

Table 7: Management Port LEDs

LED	State	Description
LINK	Glows green	Link is present.
	Blinks green	Activity.
	Off	No link is present.

Table 7: Management Port LEDs (*continued*)

LED	State	Description
TX/RX	Orange	Connection is 1000 Mbps.
	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

You use the traffic interface ports to connect the appliance to your network. The interfaces receive and forward traffic. The type and capacity of interface ports vary by model.

The following topics describe features of traffic interface ports:

- [Copper Ports on page 6](#)
- [Traffic Interface Features on page 7](#)
- [NICs Off on page 10](#)
- [Peer Port Modulation on page 11](#)

## Copper Ports

Figure 3 on page 6 shows copper port LEDs.

Figure 3: Copper Port LEDs



**NOTE:** The figure shows an IDP250 traffic interface module. The IDP75 traffic interface module is similar but has only one pair of traffic interfaces.

Table 8 on page 7 describes copper port LED states.



Table 8: Copper Port LEDs

LED	State	Description
LINK ACT	Glows green	Link is present.
	Blinks green	Activity.
	Off	No link present.
LINK SPD	Green	Connection is 100 Mbps.
	Yellow	Connection is 1 Gbps.
	Off	If LINK ACT is on, the connection is 10 Mbps. If LINK ACT is off, LINK SPD off indicates no link is present as well.
BYP	Green	Interface is not in bypass mode.
	Yellow	Interface is in bypass mode.
	Off	Interface is turned off (NICs off state).



**NOTE:** For copper interface ports, if failure or shutdown triggers NICs off state, LINK ACT and LINK SPD LEDs are turned off.

## Traffic Interface Features

Traffic interfaces are network interface cards (NICs). In the IDP Series configuration abstraction, a pair of traffic interfaces is called a virtual router. For example, virtual router vr1 comprises interface ports eth2 and eth3. For each virtual router, you use the Appliance Configuration Manager (ACM) to configure the deployment mode (sniffer or transparent) and bypass options (internal, external, or off). The following topics describe these settings:

- [Deployment Mode on page 7](#)
- [Layer 2 Bypass on page 8](#)
- [Internal Bypass on page 8](#)
- [External Bypass on page 10](#)

For guidance on using ACM to configure virtual router settings, see the ACM online help.

### Deployment Mode

You specify a deployment mode for each virtual router. You have two options:

- **Transparent**—In an in-path, transparent mode deployment, traffic arrives in one interface and is forwarded through the other. The IDP Series appliance detects attacks and takes action according to your security policy rules. You connect the IDP Series traffic interfaces to firewalls or switches in the network path.

- **Sniffer**—In an out-of-path, sniffer mode deployment, the IDP Series appliance can detect attacks but can take only limited action. You connect the IDP Series traffic interfaces to a mirrored port of a network hub or switch.

The IDP75 device has a single virtual router. Therefore, IDP75 does not support a “mixed” deployment of one or more virtual routers in transparent mode and one or more virtual routers in sniffer mode. For more information on deployment mode, see the *IDP Series Concepts and Examples Guide*.

---

### Layer 2 Bypass

You enable or disable Layer 2 bypass to determine how the IDP Series device handles Layer 2 packets.

When the IDP Series appliance is deployed in the path of network traffic, it can take three types of actions on the packets it receives:

- Drop it.
- Pass it through.
- Process it according to IDP OS rules to determine whether to drop it, forward it, rate limit, and so forth.

The IDP Series appliance processes Layer 2 traffic as follows:

- Processes address resolution protocol (ARP) and Layer 2 packets related to internet protocol (IPv4) traffic.
- Drops all other Layer 2 traffic, unless the Layer 2 bypass setting is enabled.
- When Layer 2 bypass is enabled, the IDP Series device passes through Layer 2 packets related to bypass and high availability deployments (such as heartbeats or Bridge Protocol Data Unit (BPDU) packets), and non-IPv4 packets and packets related to switching and routing protocols, such as IPv6, internetwork packet exchange (IPX), Cisco Discovery Protocol (CDP), and interior gateway routing protocol (IGRP), and so forth.

The IDP Series appliance processes TCP/IP traffic according to implicit rules related to traffic anomaly detection and explicit rules specified in the security policy.

---

### Internal Bypass

The Internal Bypass feature is intended for deployments where a network security policy privileges availability over security. In the event of failure or graceful shutdown, traffic bypasses the IDP processing engine and is passed through the IDP Series device uninspected.

The Internal Bypass feature operates through a timing mechanism. When enabled, the timer on traffic interfaces counts down to a bypass trigger point. When the IDP Series appliance is turned on and available, it sends a reset signal to the traffic interface timer so that it does not reach the bypass trigger point. If the IDP OS encounters failure, then it fails to send the reset signal, the timer counts down to the trigger point, and the traffic

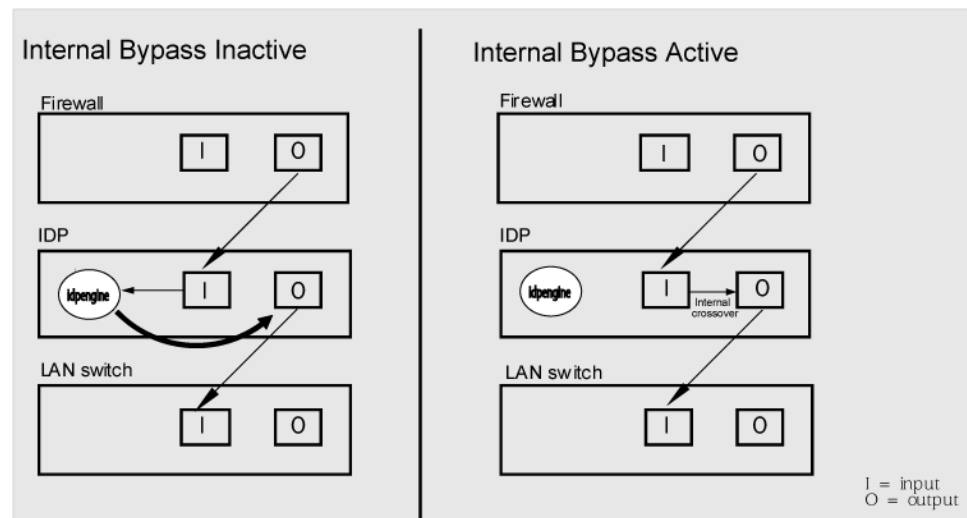
interfaces enter a bypass state. If the IDP Series appliance is shut down gracefully, the traffic interfaces immediately enter bypass.

With copper NICs, the bypass mechanism joins the interfaces mechanically to form a circuit that bypasses IDP processing. Packets traverse the IDP Series device as if the path from eth2 (receiving interface) to eth3 (transmitting interface) were a crossover cable. No packet inspection or processing occurs.

With fiber NICs, the bypass mechanism uses optical relays instead of copper relays. During normal operations, the optical relays send light to the built-in optical transceivers. When bypass is triggered, the relays flip state, and the light signal is redirected to optically connect the two external ports.

Figure 4 on page 9 compares the data path when Internal Bypass is enabled but not activated with the data path when Internal Bypass is activated.

**Figure 4: Internal Bypass**



When the IDP OS resumes healthy operations, it sends a reset signal to the traffic interfaces, and the interfaces resume normal operation.



**NOTE:** All copper port traffic interfaces support internal bypass. Some, but not all, fiber port traffic interfaces support internal bypass. Check with your sales contact for applicable part numbers.



**NOTE:** Bypass settings are applicable only for deployments where the virtual router is in the network path—transparent mode deployments.

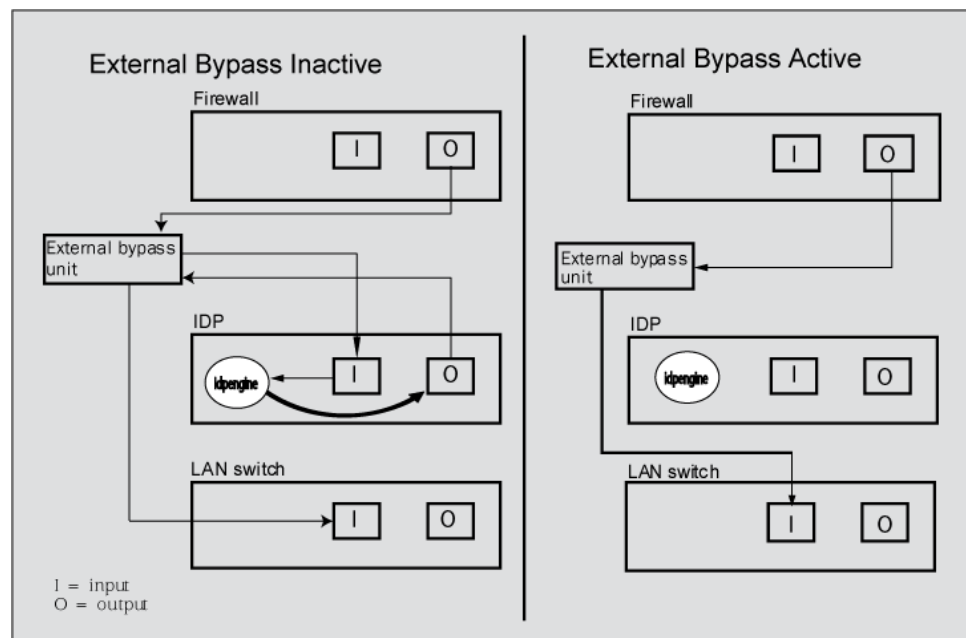


**NOTE:** The bypass and PPM features are applied independently. The Internal Bypass setting is related to the *status of the IDP operating system*. The peer port modulation setting is related to the *status of the link*. It is possible to have a healthy operating system and a link with status down, or a failed operating system and a link with status up.

### External Bypass

The External Bypass setting supports third-party external bypass units. Deployments with external bypass units depend on the functionality of the external bypass unit to check the status of the IDP Series appliance and make the determination whether to send packets through or around the IDP Series device. Most external bypass units test for availability by sending heartbeat packets through the device. If the packets reach the expected destination, the external bypass unit allows the traffic to continue through the IDP Series appliance. If the packets fail to reach the expected destination, the external bypass unit determines the IDP Series is unavailable, so it forwards traffic around the IDP Series device. The IDP Series supports external bypass solutions by allowing the heartbeat traffic to pass through the device regardless of the Layer 2 Bypass setting. In other words, if you disable Layer 2 Bypass and enable External Bypass, most Layer 2 traffic will be dropped but the heartbeat traffic used in the external bypass deployment will be passed through. [Figure 5 on page 10](#) compares the data path when External Bypass is enabled but not activated with the data path when External Bypass is activated.

Figure 5: External Bypass



### NICs Off

The NICs Off setting is intended to support network security policies that privilege security over availability—you want the network path to be unavailable if the IDP Series device

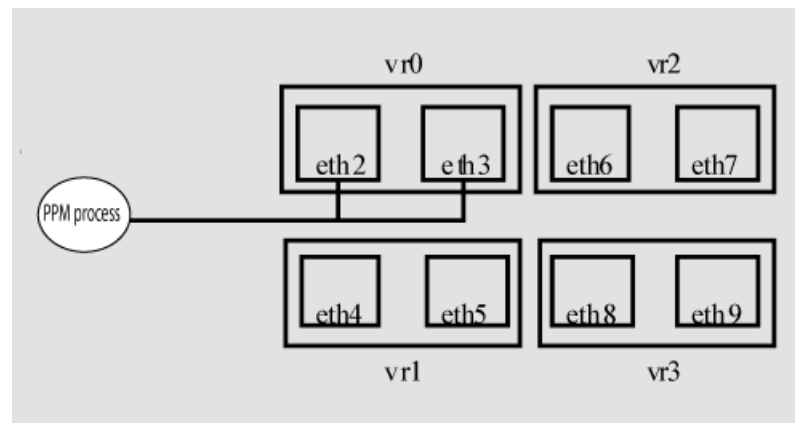
is in a state in which it cannot inspect the traffic. With NICs Off configured, in the event of failure or graceful shutdown, the interfaces are turned off and the IDP Series appliance becomes a point of failure. If your network design includes redundant network paths, you can configure your routers to detect the downed IDP Series interfaces and choose an alternate path.

## Peer Port Modulation

The peer port modulation (PPM) feature supports deployments where routers monitor link state to make routing decisions. In these deployments, a router might be set to monitor link state on only one side of the IDP Series appliance. Suppose, for example, the router monitors only the inbound interface. Suppose the inbound interface remains up but the outbound interface goes down. The router watching the inbound link would detect an available link and forward traffic to the IDP Series appliance. Traffic would be dropped at the point of failure—the outbound link. PPM propagates a link loss state for one traffic interface to all interfaces in the IDP Series virtual router.

When PPM is enabled, a PPM daemon monitors the health of IDP Series traffic interfaces belonging to the same virtual router. If a traffic interface loses link, the PPM process turns off any associated network interfaces in the same virtual router so that other network devices detect that the virtual router is down and route around it. For example, assume you have enabled PPM and configured IDP Series virtual routers as shown in [Figure 6 on page 11](#).

**Figure 6: Peer Port Modulation**



Suppose there is a network problem and eth3 goes down. The PPM daemon detects this and turns off the other interface in vr0: eth2. The interfaces in vr1, vr2, and vr3 are unaffected. After you fix the problem with eth3, the PPM daemon detects this, and turns on eth2.



.....

**NOTE:** The PPM feature is independent of the bypass feature (NIC state setting). PPM is related to the *status of the link*, not the status of the IDP operating system. A link can be down even when the IDP operating system is healthy. Note, however, that PPM runs as a control plane process and operates only when the IDP Series appliance is turned on and the control plane is available. If the IDP operating system is unavailable, the PPM feature is also unavailable, regardless of the setting for the NIC state.

.....

## CHAPTER 2

# Software Overview

This chapter includes the following topics:

- [On-Box Software Overview on page 13](#)
- [Centralized Management with NSM Overview on page 14](#)
- [J-Security Center Updates Overview on page 15](#)

## On-Box Software Overview

---

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

[Table 9 on page 13](#) summarizes the IDP Series on-box management software and utilities.

**Table 9: IDP Series On-Box Utilities**

Software	Usage
EasyConfig	<p>When you install a new appliance, you can use the EasyConfig script to assign the appliance an IP address and initialize a simple configuration.</p> <p>To run the EasyConfig script, connect to the serial port console.</p>
QuickStart	<p>When you install a new appliance, you can use QuickStart to deploy the appliance with the default virtual router configured in either sniffer or transparent mode and all configuration defaults.</p> <p>To access QuickStart, connect to the management interface and open the QuickStart URL in your browser.</p>
ACM	<p>When you install a new appliance, you can use ACM to configure the network settings, network interfaces, and user access.</p> <p>To access ACM, connect to the management interface and open the ACM URL in your browser.</p>
scio utility	<p>You can use the <b>scio</b> utility to get or set appliance configuration information.</p> <p>For details, see the <i>IDP Series Administration Guide</i>.</p>

Table 9: IDP Series On-Box Utilities (*continued*)

Software	Usage
idp.sh utility	<p>You can use the <b>idp.sh</b> utility to start, stop, or get status information on appliance processes.</p> <p>For details, see the <i>IDP Series Administration Guide</i>.</p>
sctop utility	<p>You can use the <b>sctop</b> utility to monitor connection tables and view status.</p> <p>For details, see the <i>IDP Series Administration Guide</i>.</p>
bypassStatus utility	<p>You can use <b>bypassStatus</b> commands to display settings for the daemon that monitors traffic interface NIC state.</p> <p>For details, see the <i>IDP Series Administration Guide</i>.</p>
IDP Reporter	<p>You can use the IDP Reporter to view statistics on attacks the IDP Series appliance has detected and responded to, as well as application volume tracking (AVT) statistics.</p> <p>For details, see the <i>IDP Reporter User's Guide</i>.</p>

## Centralized Management with NSM Overview

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 appliances, and IC Series appliances. You typically deploy NSM in a management subnet accessible to the NSM-managed devices.

Figure 7 on page 14 illustrates the flow of information between the tiers of the central management solution: the NSM user interface, the NSM server, and IDP Series appliances.

Figure 7: IDP Series-NSM Communication



The IDP Series 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 Series appliances, and between the NSM server and the NSM user interface, is encrypted and authenticated.



For IDP Series deployments, centralized management provides the following benefits:

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

For information about installing NSM and using NSM distributed management features, management objects (such as address objects, service objects, and templates), and navigational and display features, see the NSM documentation.

## 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 software, 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 Series Administration Guide*.



## PART 2

# Performing the Installation

- [Installation Overview on page 19](#)
- [Installing the Appliance to Your Equipment Rack and Connecting Power on page 21](#)
- [Performing the Initial Network Configuration and Licensing Tasks on page 25](#)
- [Connecting the IDP Series Traffic Interfaces to Your Network and Verifying Traffic Flow on page 31](#)



## CHAPTER 3

# Installation Overview

This chapter includes the following topics:

- [Before You Begin on page 19](#)
- [Basic Steps on page 20](#)

### 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 appliance 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.

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

## Basic Steps

---

Take the following basic steps to install the appliance and connect it to your network:

1. Read the release notes for your release. Release notes make you aware of supported and unsupported features, known issues, and fixed issues. Go to <http://www.juniper.net/techpubs/software/management/idp/> and download the release notes for your release.
2. Become familiar with the safety and security guidelines that pertain to your installation. See “Before You Begin” on page 19.
3. Decide on the physical location for the appliance. The location depends on your deployment mode, the location of your network devices, and compliance with your company security policy.
4. Install the appliance into your equipment rack. See Rack Mounting Kits and Required Tools.

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

5. Connect power cables and power on. See Connecting Power.
6. Perform the initial configuration steps. See “Performing the Initial Configuration” on page 25.
7. Install the appliance license key. See “Installing the Product License Key” on page 29.



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

8. Connect the appliance to your network. See “Guidelines for Connecting IDP Interfaces to Your Network Devices” on page 31.
9. Verify connectivity. See “Verifying Traffic Flow” on page 34.
10. In NSM, add the IDP Series appliance to the NSM device manager. See “Adding a Reachable IDP Device to NSM” on page 39.
11. Upgrade the IDP software to the current release, update the IDP detector engine firmware, and update the NSM attack object database. See “Updating Software (NSM Procedure)” on page 47.

## CHAPTER 4

# Installing the Appliance to Your Equipment Rack and Connecting Power

This chapter includes the following topics:

- [Rack Mounting Kits and Required Tools on page 21](#)
- [Mounting to Midmount Brackets on page 22](#)
- [Mounting to Rack Rails on page 23](#)
- [Connecting Power on page 23](#)

## Rack Mounting Kits and Required Tools

[Table 10 on page 21](#) describes the rack mounting hardware included in a standard shipment and required tools that are not included in a standard shipment.

**Table 10: Rack Mounting Hardware and Required Tools**

Hardware	Description
Rack mounting kit	<p>The standard shipment for 1 RU models includes a single pair of mounting brackets/ears. Use the brackets as follows:</p> <ul style="list-style-type: none"><li>• Position the brackets in the front position to front-mount.</li><li>• Position the brackets in the middle position to midmount.</li></ul> <p>If you require additional rack mounting hardware, such as rack rails, contact your sales representative for details on rack mounting kits to suit your needs. The part number for the standard rail kit is UNIV-MR1U-RAILKIT.</p>
Required tools	<p>The following tools are not included in the standard shipment and are required to install the appliance into an equipment rack:</p> <ul style="list-style-type: none"><li>• Number 2 Phillips-head screwdriver</li><li>• Rack-compatible screws</li></ul>

### Related Documentation

- [Mounting to Midmount Brackets on page 22](#)
- [Mounting to Rack Rails on page 23](#)

## Mounting to Midmount Brackets

---

To mount the appliance using the midmount brackets:

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

**Figure 8: 1-RU Midmount Bracket**



2. With another person, 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. Secure the chassis to the rack with the rack screws.

### Related Documentation

- [Rack Mounting Kits and Required Tools on page 21](#)



## Mounting to 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.

**Figure 9: Rail with Hinged Rear Bracket**



2. Rotate the hinges on both rails so that they allow the device to slide into the rack.
3. With another person, 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.

### Related Documentation

- Rack Mounting Kits and Required Tools

## Connecting Power

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

To connect power:

1. Connect the power cable (provided) 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.



## CHAPTER 5

# Performing the Initial Network Configuration and Licensing Tasks

This chapter includes the following topics:

- [Performing the Initial Configuration on page 25](#)
- [Getting Started with the EasyConfig Wizard \(Serial Console Port\) on page 27](#)
- [Getting Started with the QuickStart Wizard \(Management Port\) on page 28](#)
- [Getting Started with the ACM Wizard \(Management Port\) on page 29](#)
- [Installing the Product License Key on page 29](#)

## Performing the Initial Configuration

---

We recommend the following workflow 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.
2. From your desk, run the ACM wizard from your Web browser. 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 11 on page 26](#) summarizes the getting started configuration tools.

Table 11: Getting Started Configuration Tools

Getting Started Tool	You Specify:	Defaults Applied:
EasyConfig wizard (Serial port)	<ul style="list-style-type: none"> <li>• Management interface IP address and netmask</li> <li>• Default route</li> <li>• Time zone, date, and time</li> <li>• Deployment mode (sniffer or transparent) for the default virtual router(s)</li> </ul>	<ul style="list-style-type: none"> <li>• Root password: abc123</li> <li>• Fully qualified domain name: Blank</li> <li>• RADIUS support: Disabled</li> <li>• Network interfaces: Auto-negotiate speed/duplex</li> <li>• Virtual routers: <ul style="list-style-type: none"> <li>• Sniffer mode: One virtual router (vr0)</li> <li>• Transparent mode: One virtual router for each pair of interfaces</li> </ul> </li> <li>• NIC State: NICs off</li> <li>• DNS: Disabled</li> <li>• NTP: Disabled</li> <li>• SSH on management port: Enabled</li> <li>• Start the ACM process when the appliance starts up: Enabled</li> </ul>
QuickStart wizard (Management port)	Same as EasyConfig Wizard.	Same as EasyConfig Wizard.
ACM wizard (Management port)	<ul style="list-style-type: none"> <li>• Management interface IP address and netmask</li> <li>• Passwords for root and admin</li> <li>• Fully qualified domain name</li> <li>• Traffic interface configuration (speed/duplex, NIC states, route table)</li> <li>• Virtual routers: deployment mode (sniffer or transparent) and NIC bypass (internal, external, or NICs off)</li> <li>• Peer port modulation</li> <li>• Layer 2 bypass (pass-through)</li> <li>• Network services (DNS, NTP, RADIUS, SSH)</li> <li>• ACM access</li> <li>• NSM connection information</li> <li>• One-time password (OTP) for interoperability with Juniper Networks SA Series or UAC devices</li> </ul>	

**Related Documentation**

- [Getting Started with the EasyConfig Wizard \(Serial Console Port\) on page 27](#)
- [Getting Started with the QuickStart Wizard \(Management Port\) on page 28](#)
- [Getting Started with the ACM Wizard \(Management Port\) on page 29](#)

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



**NOTE:** After you have completed the initial configuration, we highly recommend that you use ACM to change the default password.

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 and 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 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 appliance.

**Related Documentation** • [Performing the Initial Configuration on page 25](#)

---

## 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 the user 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.

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.

**Related Documentation** • [Performing the Initial Configuration on page 25](#)

## Getting Started with the ACM Wizard (Management Port)

You use the ACM wizard to complete the appliance 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.

**Related Documentation** • [Performing the Initial Configuration on page 25](#)

## Installing the Product License Key

IDP OS 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 OS command-line interface:
  - Use SSH to connect to the IP address or hostname for the management interface. Log in as **admin** and enter **su –** to switch to **root**.
  - If you prefer, make a connection through the serial port and log in as **root**.
5. Use SCP or FTP to copy the license file to the IDP Series appliance. The IDP Series appliance does not run an FTP server, so you have to initiate the FTP session from the IDP Series appliance.

6. Change directory to the temporary directory:

```
[root@localhost ~] cd /tmp
```

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

```
[root@localhost ~] chmod 777 lic.txt
```

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

```
[root@localhost ~] scio lic add lic.txt
```

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

```
[root@localhost ~] scio lic list
[root@localhost ~]# scio lic list
ID Machine ID      Issue Date          Expiration          OK
Feature
-----
1 Upgrade          Tue Apr 25 00:00:00 2006 Sat Apr 25 00:00:00 2009 Y
idp_key
[root@localhost ~]#
```

**Related Documentation**

- [Basic Steps on page 20](#)



## CHAPTER 6

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

This chapter includes the following topics:

- [Guidelines for Connecting IDP Series Interfaces to Your Network Devices on page 31](#)
- [Choosing Cables for Traffic Interfaces \(Copper Ports\) on page 32](#)
- [Connecting and Disconnecting Fiber Cables on page 33](#)
- [Verifying Traffic Flow on page 34](#)

### Guidelines for Connecting IDP Series Interfaces to Your Network Devices

---

We recommend you deploy the IDP Series appliance between gateway firewalls and DMZ or internal networks.

[Table 12 on page 31](#) provides guidelines for connecting IDP Series interfaces to your network.

**Table 12: Interface Connection Guidelines**

Port	Cable Connection Guidelines
Management port	<p>NSM must be able to reach the IDP Series appliance through this connection.</p> <ol style="list-style-type: none"><li>1. Connect one end of a CAT-5 cable into the MGMT port located at the front of the chassis.</li><li>2. Connect the other end to a switch or hub (recommended) in your network.</li></ol>

---

Table 12: Interface Connection Guidelines (*continued*)

Port	Cable Connection Guidelines
Traffic interface ports	<b>Sniffer Mode – Copper Ports</b> <ol style="list-style-type: none"> <li>1. Connect one end of a CAT-5 straight-through cable to a traffic interface port located at the front of the chassis.</li> <li>2. Connect the other end to the Switched Port Analyzer (SPAN) port of a switch or a hub.</li> </ol>
	<b>Sniffer Mode – Fiber Ports</b> <ol style="list-style-type: none"> <li>1. Connect one end of an LC fiber cable to either one of the ports of a traffic interface pair.</li> <li>2. Connect the other end of the cable to the corresponding port of the switch.</li> </ol>
	<b>Transparent Mode – Copper Ports</b> <ol style="list-style-type: none"> <li>1. Connect one end of a CAT-5 straight-through cable to a traffic interface port located at the front of the chassis.</li> <li>2. Connect the other end to the corresponding port of a firewall, switch, or server.</li> <li>3. Connect one end of a CAT-5 cable to the outbound port of a traffic interface pair (for example, eth3).</li> <li>4. Connect the other end to a corresponding the corresponding port of a firewall, switch, or server.</li> </ol>
	<b>Transparent Mode – Fiber Ports</b> <ol style="list-style-type: none"> <li>1. Connect one end of an LC fiber cable to the inbound port of a traffic interface pair.</li> <li>2. Connect the other end to the corresponding port of the switch.</li> <li>3. Connect one end of an LC fiber cable to the outbound port of a traffic interface pair.</li> <li>4. Connect the other end to the corresponding port of the switch.</li> </ol>

- Related Documentation**
- [Choosing Cables for Traffic Interfaces \(Copper Ports\) on page 32](#)
  - [Connecting and Disconnecting Fiber Cables on page 33](#)
  - [Verifying Traffic Flow on page 34](#)

## Choosing Cables for Traffic Interfaces (Copper Ports)

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

- [Connecting Devices That Support Auto-MDIX on page 33](#)
- [Connecting Devices That Do Not Support Auto-MDIX on page 33](#)
- [Connecting Devices to Support Internal Bypass on page 33](#)

## 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.



**NOTE:** IDP75, IDP250, IDP800, and IDP8200 support auto-MDIX.

## 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.



**NOTE:** 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 Series appliance 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 the IDP Series appliance and a straight-through cable between the IDP Series appliance and the switch. When internal bypass activates and crosses-over the connection between the IDP Series 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 procedures 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. 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.
3. 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. 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.
2. 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.
3. Gently but firmly pull the clip from the transceiver port.

---

## Verifying Traffic Flow

**Purpose** After you have installed the appliance, run the initial network configuration, and connected the appliance to your network, you can perform the following procedure to verify traffic flows through the appliance.

**Action** To verify that traffic is flowing through the appliance:

1. Make sure the appliance is connected to a live traffic feed.
2. Connect to the IDP OS command-line interface:
  - Use SSH to connect to the IP address or hostname for the management interface. Log in as **admin** and enter **su –** to switch to **root**.
  - If you prefer, make a connection through the serial port and log in as **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	08/09/2006 03:08:07
ICMP	3	0	0	0	08/08/2006 18:03:51
UDP	3386	3	1	7	08/08/2006 19:31:01
TCP	151164	12	6	9	08/09/2006 07:01:36

Changes in the UDP and TCP flow and session counts indicate traffic is flowing through the appliance.

**Related Documentation**

- [Basic Steps on page 20](#)



## PART 3

# Adding the IDP Series Device to NSM

- [Adding the IDP Series Device to NSM on page 39](#)





## CHAPTER 7

# Adding the IDP Series Device to NSM

This chapter includes the following topics:

- [Reviewing Compatibility with NSM on page 39](#)
- [Adding a Reachable IDP Series Device to NSM on page 39](#)

## Reviewing Compatibility with NSM

---

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

In some cases, you might be required to install a schema update on NSM to support the IDP Series release. If so, follow the instructions in the release notes to install the schema update.



**NOTE:** The schema update is also known as the *forward support update*.

### Related Documentation

- [Adding a Reachable IDP Device to NSM on page 39](#)

## Adding a Reachable IDP Series Device to NSM

---

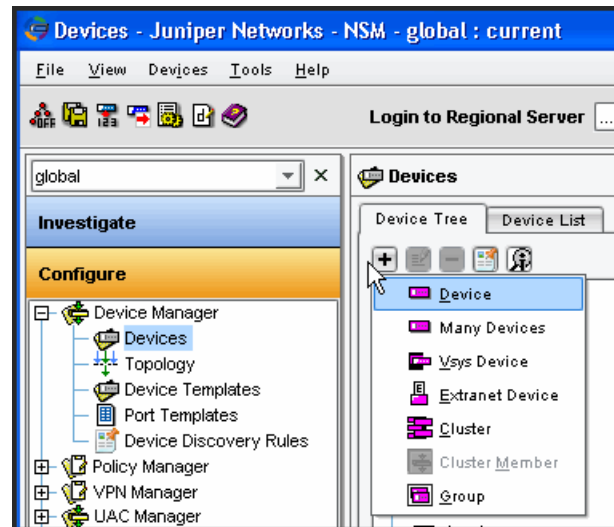
This procedure assumes the IDP Series device is reachable. A reachable device is a device you have installed and initialized, including configuring an IP address for the management interface and connecting the management interface to the network. You complete the reachable device workflow in cases where you set up the IDP Series appliance first and add it to NSM second.

For information on a workflow where you add the device to NSM first and set up the IDP Series appliance second, see the *IDP Series Administration Guide*.

To import an IDP Series device with a known IP address:

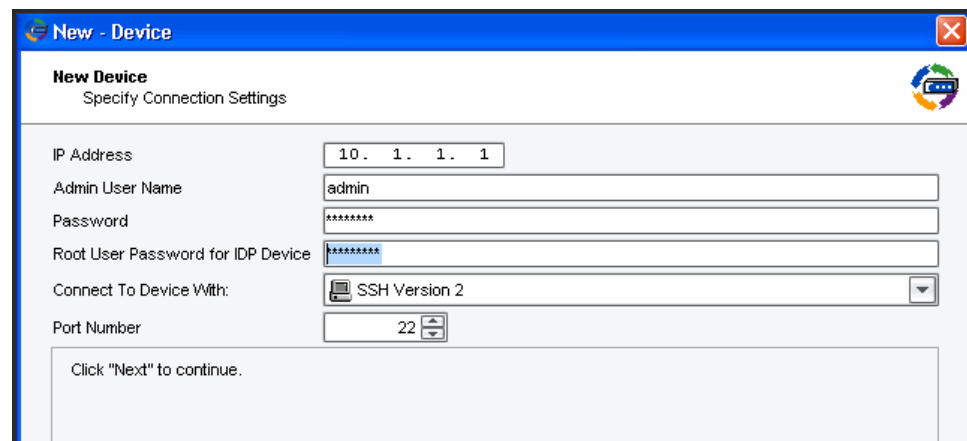
1. In the NSM navigation tree, select **Device Manager > Devices**.

Figure 10: NSM Add Device Wizard: Add Device



2. Click the + icon and select **Device** to display the Add Device wizard.
3. Select **Device Is Reachable** (default) and click **Next** to display the page where you configure connection settings.

Figure 11: NSM Add Device Wizard: Connection Settings



4. In the Specify Connection Settings dialog box, enter the following connection information:
  - Enter the IP address of the IDP Series device.
  - Enter **admin** for the username of the device admin user.
  - Enter the password for the device admin user. You set the password for admin when you ran the ACM Wizard.

- Enter the password for the device root user. You set the password for root when you ran the ACM Wizard.



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

- Select **SSH Version 2** and port 22.

Click **Next**.

The Wizard displays a page where you can verify the integrity of the connection between the IDP Series appliance and NSM. Please wait a moment as the NSM retrieves SSH key fingerprint information from the IDP Series appliance.

Figure 12: NSM Add Device Wizard: SSH Key Fingerprint Information

<b>New Device</b> Verify Device Authenticity
Device SSH Key f4:91:d0:04:b7:61:00:77:45:c3:cc:bd:af:b3:5b:a2
Click "Next" to Accept the Device SSH Key

5. Log into the IDP OS 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 OS command-line interface:
    - Use SSH to connect to the IP address or hostname for the management interface. Log in as **admin** and enter **su –** to switch to **root**.
    - If you prefer, make a connection through the serial port and log in as **root**.
  - b. Enter **cd /etc/ssh**.
  - c. Enter **ssh-keygen -l -f ssh\_host\_dsa\_key**.

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
```

After you have verified the SSH key fingerprint matches, click **Next**.

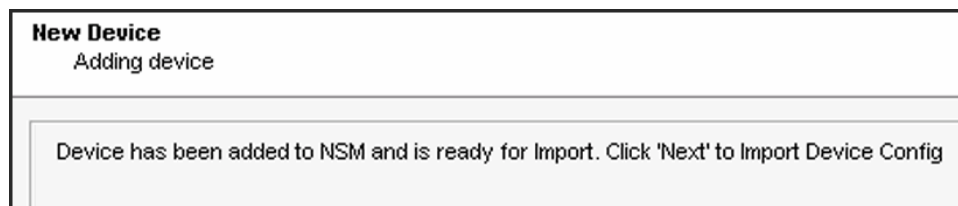
The Wizard displays a page where NSM retrieves and displays inventory information. Please wait a moment as the NSM retrieves inventory information from the IDP Series appliance.

Figure 13: NSM Add Device Wizard: Inventory Information

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...	

6. Verify that the device type, OS version, device serial number, and device mode are correct.
7. Click **Next** to add the device to NSM. Upon success, NSM displays the following message:

Figure 14: NSM Add Device Wizard: Add Device Confirmation



8. Click **Next** to import the configuration from the IDP Series device. Upon success, NSM displays the following message:

Figure 15: NSM Add Device Wizard: Configuration Import Confirmation



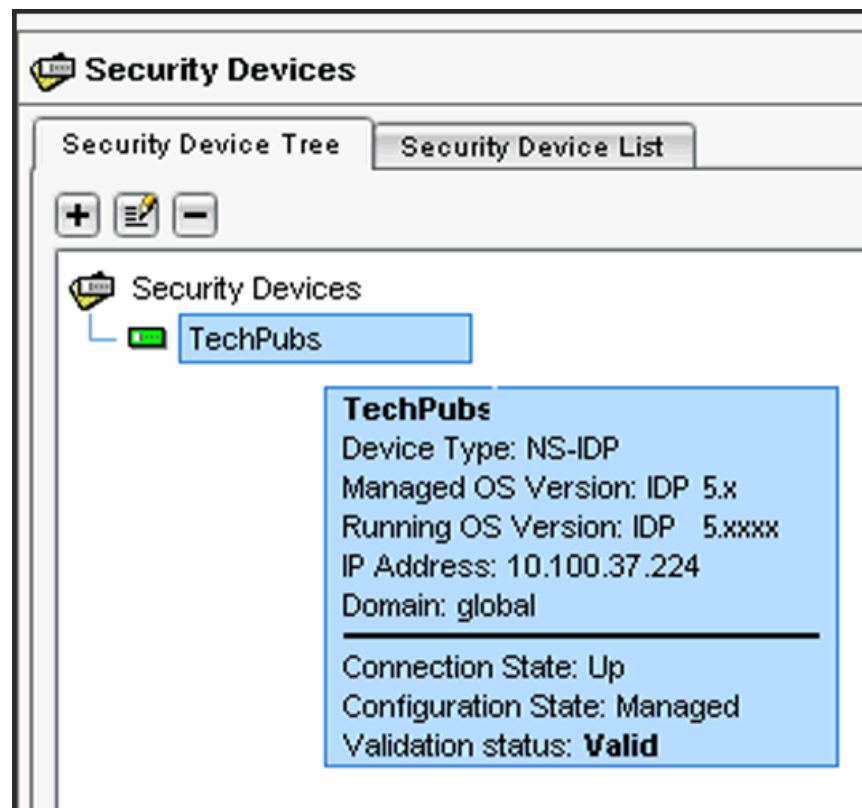
9. Click **Finish**.

For IDP OS 4.1 and later devices, NSM next runs a job to update the IDP device with the Recommended IDP security policy. The Job Information dialog box shows the status of the Update Device job.

10. After the job is complete, double-click the device in Device Manager to view the imported configuration.

To check the device configuration status, mouse over the device and verify that the device status displays **Managed**.

Figure 16: NSM Device Manager: Viewing Device Status



- Related Documentation**
- [Reviewing Compatibility with NSM on page 39](#)
  - [Basic Steps on page 20](#)

## PART 4

# Upgrading Software

- [Upgrading Software on page 47](#)
- [Reimaging the Appliance on page 51](#)





## CHAPTER 8

# Upgrading Software

This chapter includes the following topics:

- [Updating Software \(NSM Procedure\) on page 47](#)
- [Upgrading Software \(CLI Procedure\) on page 49](#)

### Updating Software (NSM Procedure)

---

To update IDP software:

1. Add the IDP software to the NSM GUI server.
2. Push the IDP software from the NSM GUI server to one or more IDP devices.

To add an IDP software image to the NSM GUI server:

1. Download the software image:
  - a. Go to <https://www.juniper.net/customers/csc/software/> and log in with your customer username and password.
  - b. Enter the IDP Series device serial number to display a view of applicable software releases available for download.
  - c. Click the applicable link to display the software download page.
  - d. Download the software to a location you can access from your NSM client.
2. From the NSM main menu, select **Tools > Software Manager** to display the Software Manager dialog box.
3. Click the + button to display the Open dialog box.
4. Select the IDP software image you just downloaded and click **Open** to add the software image to the NSM GUI server.
5. Click **OK**.

To push the software image from the NSM GUI server to IDP Series devices:

1. From the NSM main menu, select **Devices > Software > Install Device Software** to display the Install Device Software dialog box.
2. From the Select OS Name list, select **ScreenOS/IDP**.
3. From the Select Software Image list, select the image file you just added to the NSM GUI server.
4. In the Select Devices list, select the IDP Series devices on which to install the software update.
5. Click **Next** and complete the wizard steps.
6. Select **Automate ADM Transformation** to automatically update the Abstract Data Model (ADM) for the device after NSM installs the update.



**NOTE:** If you clear this setting, the update is installed onto the device, but you cannot manage the device from NSM until the device ADM is updated.

7. Click **Finish** to display upgrade status in the Job Information dialog box.
8. When the upgrade finishes, click **Close** to exit the Job Information dialog box.
9. In the NSM Device Manager, right-click the IDP Series device and select **Import Device**.

The software upgrade is complete.

- Next Steps:**
1. 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.

2. Push the updated IDP detector engine to IDP Series devices:

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



**NOTE:** Updating the IDP detector engine on a device does not require a reboot of the device.

3. Push a security policy update job to update attack objects in use in your security policy:
  - a. In NSM, select **Devices > Configuration > Update Device Config**.
  - b. Select devices to which to push the updates and set update job options.
  - c. Click **OK**.

**Related Documentation** • [Upgrading Software \(CLI Procedure\) on page 49](#)

## Upgrading Software (CLI Procedure)

To upgrade IDP software from the CLI:

1. Download the software image to a host that runs an FTP server. Follow these steps:
  - a. Go to <https://www.juniper.net/customers/csc/software/> and log in with your customer username and password.
  - b. Navigate to **IDP > ScreenOS Software Downloads (including NSM/Global Pro, STRM, IDP and NetScreen-Remote)**. In the row for IDP OS, click **5.1**.
  - c. Save the **sensor\_version.sh** file (where version is the number that identifies the software release version).
2. Connect to the IDP OS command-line interface in one of the following ways:
  - Use SSH to connect to the IP address or hostname for the management interface. Log in as **admin** and enter **su -** to switch to **root**.
  - If you prefer, make a connection through the serial port and log in as **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 license file to the IDP Series appliance. The IDP Series appliance does not run an FTP server, so you have to initiate the FTP session from the IDP Series appliance.
4. Run the upgrade script by entering **sh sensor\_version.sh**, where *version* is the number that identifies the software release version. When the script has finished, enter **reboot**.
5. In the NSM Device Manager, right-click the device, select **Adjust OS Version**, and complete the wizard steps.
6. In the NSM Device Manager, right-click the IDP Series device and select **Import Device**.

The software upgrade is complete.

**Next Steps:** 1. Download the IDP detector engine and NSM attack database updates to the NSM GUI server:

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

2. Push the updated IDP detector engine to IDP Series devices:

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



---

**NOTE:** Updating the IDP detector engine on a device does not require a reboot of the device.

---

3. Push a security policy update job to update attack objects in use in your security policy:
  - a. In NSM, select **Devices > Configuration > Update Device Config**.
  - b. Select devices to which to push the updates and set update job options.
  - c. Click **OK**.

**Related  
Documentation**

- [Updating Software \(NSM Procedure\) on page 47](#)

## CHAPTER 9

# Reimaging the Appliance

This chapter includes the following topic:

- [Reimaging and Relicensing an Appliance on page 51](#)

### Reimaging and Relicensing an Appliance

The appliance comes with software preinstalled. If needed, you can reinstall the factory image. This process is known as *reimaging* the appliance. The reimaging process rewrites the disk except for the partition containing `/var/idp`. If necessary and if possible, you should save a copy of data or custom configuration files before reimaging.

If you reimage the appliance, you must also relicense it.

To reimage the appliance:

1. Connect a PC to the console serial port of the device, using the serial cable provided with the appliance.
2. Power off the appliance.
3. Insert the USB flash memory stick that shipped with the appliance into the USB port on the front of the appliance. If you have misplaced your USB flash memory stick, contact Juniper Networks Technical Assistance Center (JTAC). The part number for the USB flash memory stick is IDP-FLASH (IDP75, IDP250, IDP800) or IDP-FLASH-8200 (IDP8200).
4. Power on the appliance.

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

5. When the reimaging process has completed, remove the USB stick and reboot.

#### **Next Steps**

1. Configure the appliance as if a new installation.
2. Relicense the appliance.
3. Re-add the appliance to NSM.
4. Push updates to detector engine, attack object, and security policy.

**Related  
Documentation**

- [Performing the Initial Configuration on page 25](#)
- [Installing the Product License Key on page 29](#)
- [Adding a Reachable IDP Device to NSM on page 39](#)

## PART 5

# Technical Specifications and Compliance Statements

- [Technical Specifications on page 55](#)
- [Compliance Statements on page 57](#)





## CHAPTER 10

# Technical Specifications

This chapter includes the following topics:

- [IDP75 Technical Specifications on page 55](#)

### **IDP75 Technical Specifications**

---

[Table 13 on page 55](#) lists physical specifications.

**Table 13: Physical Specifications**

Specification	Value
Form Factor	1 RU
Height	1.69 in. (4.3 cm)
Width	17 in. (43.2 cm)
Depth	15 in. (38.1 cm)
Weight	15 lb (6.80 kg)

[Table 14 on page 55](#) lists power specifications.

**Table 14: Power Specifications**

Specification	Value
AC input voltage	100 to 240 VAC
AC input line frequency	50 to 60 Hz
AC input current	4.0 to 2.0 A
Maximum power	200 W

[Table 15 on page 56](#) lists power cord specifications.

**Table 15: Power Cord Specifications**

Country	Specifications
United States and Canada	<ul style="list-style-type: none"> <li>• UL-approved and CSA-certified</li> <li>• Flexible cord minimum spec: No. 18 (1.5 mm<sup>2</sup>SVT or SJT, 3-conductor</li> <li>• Current capacity of 10A minimum</li> <li>• Earth-grounding attachment plug with NEMA 5-15P (10A, 125V) configuration</li> </ul>

[Table 16 on page 56](#) list environmental specifications.

**Table 16: Environmental Specifications**

Specification	Value
Operating temperature	41° to 104° F (5° to 40° 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)	10,000 ft (3,048 m)
Altitude (storage)	40,000 ft (12,192 m)

Heat dissipation rates depend on the traffic rate and the number and type of features you have enabled. [Table 17 on page 56](#) provides guidelines.

**Table 17: Heat Dissipation Guidelines**

Specification	Watts	BTU/hour
Minimum	55	188
Maximum	67	229

## CHAPTER 11

# Compliance Statements

This chapter includes the following topic:

- [Standards Compliance on page 57](#)

## Standards Compliance

---

Table 18:

Category	Standards Compliance
Safety	<ul style="list-style-type: none"><li>• UL 60950, Third Edition — Safety of Information Technology Equipment</li><li>• CSA C2.22 No. 60950, Third Edition — Safety of Information Technology Equipment</li><li>• EN 60950, 2000 — Safety of Information Technology Equipment, including Electrical Business Equipment</li><li>• IEC 60950, Third Edition — Safety of Information Technology Equipment, including Electrical Business Equipment</li></ul>
EMI	<ul style="list-style-type: none"><li>• EN 55022, 1998 Class A</li><li>• EN 61000-3-2</li><li>• FCC Part 15 Class A</li><li>• Industry Canada ICES-003 Class A</li><li>• VCCI Class A</li></ul>
Immunity	<ul style="list-style-type: none"><li>• EN 55024, 1998</li></ul>



## PART 6

# Index

- [Index on page 61](#)



# Index

## Symbols

1998 Class A compliance.....57

## A

ACM .....13, 29  
ACM Online Help.....vii  
adding a device to NSM.....39  
audience for documentation.....v  
auto-MDIX.....32

## B

BTU/hour.....55  
bypassStatus utility.....14

## C

compliance  
    EMI standards.....57  
    immunity standards.....57  
connecting power.....23  
console serial port.....5  
copper ports  
    cable guidelines.....32  
CSA C2.22 No. 60950 compliance.....57  
customer support.....viii  
    contacting JTAC.....viii

## D

DNS, setting.....26

## E

EasyConfig .....13, 27  
EMI compliance.....57  
EMI compliance specifications.....57  
EN 1998 compliance.....57  
EN 2000 compliance.....57  
EN 55022 compliance.....57  
EN 55024 compliance.....57  
EN 60950 compliance.....57  
EN 61000-3-2 compliance.....57  
environmental specifications.....55

## F

fault LEDs.....4  
FCC Part 15 Class A compliance.....57  
fiber ports  
    cables.....33

## H

hard drives  
    LEDs.....4  
heat dissipation.....55

## I

IC Series Interoperation.....26  
ICES-003 Class A compliance.....57  
IDP Administration Guide.....vii  
IDP Concepts and Examples Guide.....vii  
IDP Custom Attack Objects Reference and  
    Examples Guide.....vii  
IDP Reporter.....14  
IDP Reporter User's Guide.....vii  
IDP Series Installation Guide: IDP200, IDP600,  
    IDP1100.....vii  
idp.sh utility.....14  
IDP250 Installation Guide.....vii  
IDP75.....3  
IDP75 Installation Guide.....vii  
IDP800 Installation Guide.....vii  
IDP8200 Installation Guide.....vii  
IEC 60950 safety compliance.....57  
immunity standards.....57  
Industry Canada ICES-003 Class A compliance.....57

## L

Layer 2 bypass setting.....26  
LEDs  
    fault.....4  
    hard drive.....4  
    IDP75.....3  
    power.....4  
    traffic interface.....6

## M

management interface, choosing cable for.....31  
MDIX.....32

## N

NSM  
    specifying connection information for.....26  
    updating software with.....47

NTP, setting.....	26	technical support	
<b>O</b>		contacting JTAC.....	viii
one time password.....	26	traffic interfaces	
one-time password for IC Series/SA Series.....	26	choosing cables for.....	32
<b>P</b>		copper ports.....	32
ports		fiber ports.....	32
copper.....	32	LEDs.....	6
fiber.....	32	transparent mode	
IDP75.....	3	setting.....	26
power cord specifications.....	55	<b>U</b>	
power LEDs.....	4	UL 60950 compliance.....	57
power specifications.....	55	updating software	
power supplies		CLI procedure.....	49
connecting.....	23	NSM procedure.....	47
<b>Q</b>		USB port.....	5
QuickStart.....	13, 28	<b>V</b>	
<b>R</b>		VCCI Class A compliance.....	57
rack mounting kit.....	21	virtual routers	
RADIUS, configuring.....	26	default.....	26
reimaging the appliance.....	51		
release notes.....	vii		
RJ-45 serial port.....	5		
<b>S</b>			
SA Series interoperation.....	26		
safety compliance standards.....	57		
safety guidelines.....	19		
scio utility.....	13		
sctop utility.....	14, 34		
security guidelines.....	19		
serial port console.....	5		
sniffer mode			
setting.....	26		
specifications.....	55		
EMI compliance.....	57		
immunity.....	57		
SSH-access, configuring.....	26		
standards			
EMI compliance.....	57		
safety compliance.....	57		
support, technical See technical support			
<b>T</b>			
technical specifications.....	55		