**Juniper Networks**
**Intrusion Detection and Prevention**

# IDP 75, 250, 800, and 8200 Installation Guide

*Releases 4.1r2a and 4.2*
*April 2008*

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

Part Number: 530-023834-01

### FCC Statement

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

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

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

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

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

### Disclaimer

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

# Table of Contents

# List of Figures

# List of Tables

# About This Guide

This guide describes the physical features of Juniper Networks Intrusion Detection and Prevention (IDP) solution: the IDP 75, IDP 250, IDP 800, and IDP 8200 sensors. It also explains how to install, configure, update/reimage, and service the IDP system.

This preface has the following sections:



## Audience

This guide is intended for experienced system and network specialists.

## Conventions

The term *sensor* is used to denote an IDP 75, 250, 800, or 8200 appliance.

Table 1 defines notice icons used in this guide.

**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. |
|  | Warning | Alerts you to the risk of personal injury. |

## Documentation

This guide is shipped in the box with all new IDP sensors. It provides the basic procedures for getting your IDP system running.

With each major software release, Juniper Networks provides the IDP Documentation CD. The CD contains the documentation set in PDF format.

The IDP documentation set includes the following books:

- ***Release Notes***—Contain the latest information about features, changes, 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.*
- ***Intrusion Detection and Prevention Concepts & Examples Guide***—Explains basic concepts of the IDP system and provides examples of how to use the system.
- ***IDP 75, 250, 800, and 8200 Installation Guide*** (this manual)—Describes the hardware components of the IDP 75, 250, 800, and 8200 sensors. Provides instructions for rack-mounting, cabling, basic configuration, management server installation, and user interface installation.
- **Online Help**—Available through the IDP Appliance Configuration Manager (ACM). The online help provides explanations for sensor configuration options as well as step-by-step directions for performing common tasks.

### *Web Access for Documentation*

To view the documentation on the Web, go to:
http://www.juniper.net/techpubs/software/management/idp/

## 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/customers/support/downloads/710059.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

### *Self-Help Online Tools and Resources*

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

- Find CSC offerings: http://www.juniper.net/customers/support/
- 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 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 on the Web or by telephone.

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

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

Chapter 1

# Planning an Installation

This chapter provides an overview of IDP configuration options. This chapter has the following sections:



## Installation Roadmap

This section provides a high-level roadmap of an IDP sensor installation. With each step is a reference to more information.

1. Install the NetScreen-Security Manager (NSM) server onto a dedicated host or hosts. See the *NetScreen-Security Manager Installation Guide* for installation instructions.

2. Install the NSM GUI on a Windows or Linux client machine. See the *NetScreen-Security Manager Installation Guide* for installation instructions.

3. Decide on a place in your network for the sensor. Choose which mode you will run. See Chapter 4, “Installing the Sensor,” on page 17.

4. Install the sensor on a rack. See Chapter 4, “Installing the Sensor,” on page 17.

5. Log into the sensor using the console port to run the EasyConfig script. This script lets you specify a sensor mode, IP address, netmask, default gateway, and date or time. See “Using the Console Serial Port to Configure the Sensor” on page 22. You can use the default login name (root) and password (abc123) for the sensor.

6. (Optional) If you want to change your default login and password, change port speeds, or do more advanced configuration of the sensor, use a Web browser to log into the sensor’s Appliance Configuration Manager (ACM). You can reach it by typing https://*SensorIPAddress* in the Address or Location box of your browser.

7. Start the NSM GUI. The default login ID is **super**. Use the password you specified when you installed the NSM server.

8. Add the sensor as an object in NSM using the Add Device wizard. Select **Device Manager > Security Devices** from the left navigational pane, and then click the + button. See "Adding Your Sensor to NSM" on page 29. The Add Device Wizard creates a database entry in NSM for the sensor, imports the sensor's configuration, and loads the Juniper Networks Recommended policy onto the sensor. At that point, your sensor is actively protecting your network.

To improve the performance and accuracy of your protection, use the *IDP Concepts & Examples Guide* and the *NetScreen-Security Manager Administrator's Guide* to tailor your security policy to your network.

**NOTE:** You must update your attack objects to get the latest protection.

## IDP Configuration Basics

This section provides an introduction to IDP configuration basics. An IDP configuration consists of the following components:

- **IDP sensor placement**—Decide where to position the sensor in the network.
- **IDP sensor placement mode**—Decide to use passive or active mode when deploying your IDP sensor.
- **NetScreen-Security Manager**—Use NetScreen-Security Manager (NSM) to administer the sensor.

### *IDP Sensor Placement*

Juniper Networks IDP sensor is an ideal solution to be implemented inline between gateway firewalls and DMZ or internal networks. IDP sensor placement is an important part of the installation.

You should choose a location for your IDP sensor based on your existing network hardware and the networks you want to protect. The examples provided in this guide place the IDP sensor behind the firewall or router.

### *IDP Sensor Deployment Mode*

IDP sensors can be installed individually or in high availability (HA) clusters of two or more.

For configurations without high availability, you can deploy the IDP sensor as a passive sniffer or as an active gateway.

- **Passive Mode**—The sniffer mode is passive. In sniffer mode, the IDP is not directly involved with packet flow. While it can send resets, protection is not guaranteed as attacks may have already happened before the reset can be acted upon. In addition, attacker machines may ignore resets.

To use an IDP sensor as a passive intrusion detection system without prevention capabilities, deploy the sensor in passive sniffer mode to monitor and log network traffic. If the sensor is attached to a network switch, you must configure the switch to mirror all traffic to that port. The IDP sensor defaults to sniffer mode.

- **Active mode**—The gateway (inline) mode is active. This mode takes full advantage of IDP attack prevention capabilities and multimethod detection mechanisms.

  With inline modes, the sensor is directly involved in the packet flow. The sensor can stop attacks by dropping malicious packets before they reach their target.

  Inline sensors are typically configured in transparent mode. For other inline modes, see "Advanced Configuration" on page 43.

**NOTE:** For IDP 8200 Release 4.2, only transparent mode is available.

One step in setting up IDP on your network is to decide on a deployment mode. Figure 1 and Figure 2 illustrate the possible deployment modes and their primary advantages and disadvantages.

**Figure 1: Sniffer Mode (Passive)**

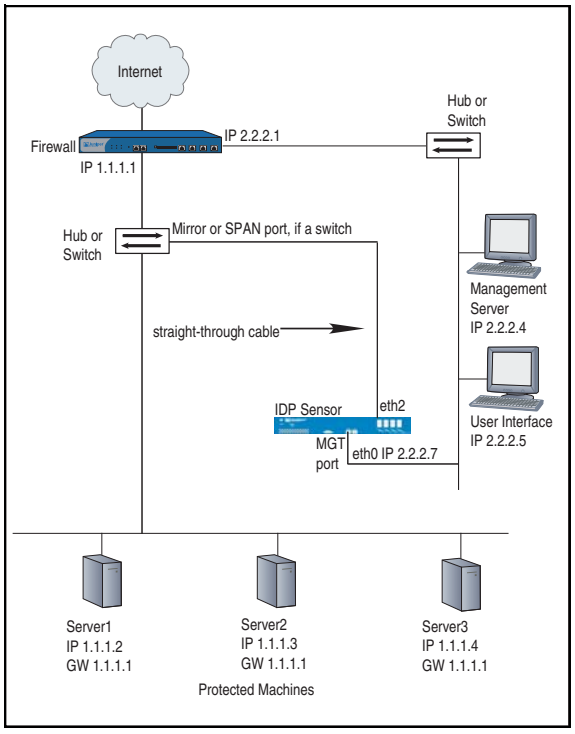



Table 2 lists the advantages and the disadvantages of using the sensor in passive sniffer mode.

**Table 2: Advantages and Disadvantages of Sniffer Mode (Passive)**

| Advantages | Disadvantages |
|---|---|
| ■ Seamlessly replaces the current intrusion detection<br>■ Causes minimal network changes<br>■ Does not create an additional point-of-failure gateway<br>■ Monitors and logs suspicious network activity | ■ Passively monitors with limited prevention only<br>■ Requires a hub or the Switched Port Analyser (SPAN) port of a switch |

**Figure 2: Transparent Mode (Inline Active)**

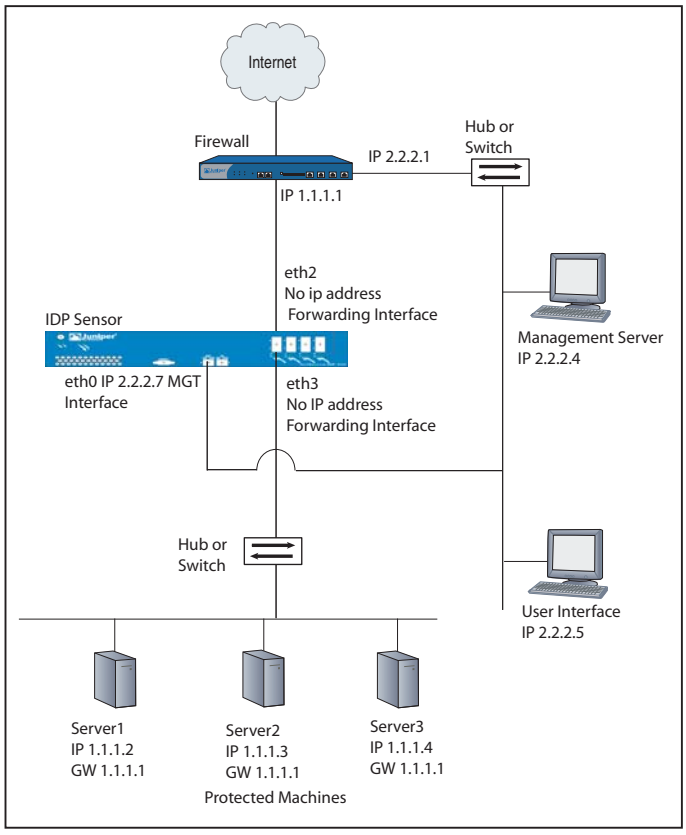



Table 3 lists the advantages and the disadvantages of using the sensor in active transparent (inline) mode.

**Table 3: Advantages and Disadvantages of Transparent Mode (Inline Active)**

| Advantages | Disadvantages |
|---|---|
| ■ Reliably responds to and prevents attacks<br>■ Simple, transparent deployment<br>■ Allows Layer 2 broadcasts<br>■ No changes to routing tables or network equipment<br>■ Forwards non-IP traffic | ■ Cannot connect IP networks with different address spaces |

## *NetScreen-Security Manager*

Use NetScreen-Security Manager to administer the sensor. See the *NetScreen-Security Manager Administrator's Guide* to tailor your security policy to your network. See the *IDP Concepts & Examples Guide* to improve the performance and accuracy of your protection.

Chapter 2

# Hardware Overview

This chapter provides detailed descriptions of the Juniper Networks IDP sensors and their components.

This chapter has the following sections:



## IDP Sensors

This section provides an overview of the following IDP sensors:



Each sensor contains a USB port you can use for reimaging the sensors.

**CAUTION:** Both the console serial port and the management network interface port use the same RJ-45 connector. Do not plug a network cable into the console serial port.

### IDP 75 Sensor

The IDP 75 sensor is optimal for small networks or low-speed network segments. Figure 3 shows the following features:

- One console serial port
- One management network interface port
- One USB port
- Two copper Ethernet ports (10/100/1000 Mbps)

**Figure 3: IDP 75 Front Panel**


### IDP 250 Sensor

The IDP 250 sensor is optimal for medium central sites or large branch offices. Figure 4 shows the following features:

- One console serial port
- One management network interface port
- One dedicated high availability port
- One USB port
- Two IOC slots (each IOC containing four gigabit ports)

**Figure 4: IDP 250 Front Panel**


### IDP 800 Sensor

The IDP 800 sensor is optimal for medium-to-large central sites or high-traffic areas. Figure 5 shows the following features:

- One console serial port
- One management network interface port
- One dedicated high availability port

- One USB port
- Two IOC slots (each IOC containing four gigabit ports)
- Two built-in copper Ethernet ports (10/100/1000 Mbps)

**Figure 5: IDP 800 Front Panel**


## *IDP 8200 Sensor*

The IDP 8200 sensor is optimal for large central sites or high-traffic areas. Figure 6 shows the following features:

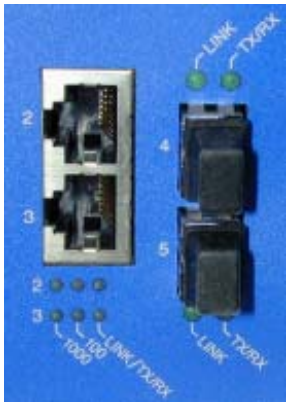
- One console serial port
- One management network interface port
- One dedicated high availability port
- One USB port
- Four IOC slots (each IOC supports 16 copper/fiber 1-Gbit ports, one 10Gbit card with copper/fiber 1Gbit ports, or two 10Gbit cards with copper\fiber 1Gbit ports)

**Figure 6: IDP 8200 Front Panel**


## Traffic Ports (Forwarding Interfaces)

The IDP 75, 250, 800, and 8200 sensors have traffic ports (forwarding interfaces), which are located on the front of each device. Sensors can have a combination of copper and fiber ports.

**Figure 7: Traffic Ports**




### *Configurable NIC States*

Copper port pairs on the IDP 75, 250, 800, and 8200 can be configured to take specified actions when the sensor becomes unavailable. Using the Appliance Configuration Manager (ACM), you can configure how the sensor responds when it is shut down gracefully and how it responds when there is a failure.

**Table 4: NIC State Options**

| ACM Settings | Modes | Availability | Description |
|---|---|---|---|
| NIC bypass | Transparent mode only | ■ Sensor failure<br>■ Graceful shutdown | While sensor is active, it does not pass NSRP packets unless Layer 2 bypass is enabled.<br>When sensor becomes unavailable, ports mechanically join in a crossover. Traffic continues to flow, but sensor does not examine traffic. |
| External bypass unit | Transparent mode only | Sensor failure only | While sensor is active, it passes NSRP packets even if Layer 2 bypass is disabled.<br>On failure, external bypass unit passes traffic around the sensor.<br>**Note:** This is a global setting. If set for any NIC, NSRP packets are allowed for all NICs. |
| NICS off | All inline modes | ■ Sensor failure<br>■ Graceful shutdown | While sensor is active, it does not pass NSRP packets unless Layer 2 bypass is enabled for transparent mode.<br>When sensor fails or when the sensor software is shut down, NICs turn off even if sensor still has power. |

## Normal State

When the IDP is active and NICs are in the normal state, NICs only pass Layer 2 traffic if in transparent mode and if Layer 2 bypass is enabled. NSRP packets are not passed, so external bypass units do not behave correctly.

## NIC Bypass State

Ethernet copper ports on the IDP 75, 250, 800, and 8200 sensors all have built-in port bypass with crossover. Port bypass only works if the sensor is configured for transparent mode. If a sensor fails or is shut down while in transparent mode, the pair of copper ports will automatically fail into a crossover “connected” state, and traffic will flow through them to and from the rest of the network without being analyzed.

NIC bypass works using a watchdog timer. Each port pair has a timer. The sensor sends each timer a reset signal every second. If a timer does not receive a reset signal for three seconds (or the configured time period), the bypass is activated. After the bypass is activated, the timer continues listening for a reset signal. When IDP becomes active again, it sends a reset signal. When the timer receives the reset signal, the bypass deactivates automatically and the sensor goes back to normal operation.

When NICs are in NIC bypass state prior to shutdown or failure, they only pass Layer 2 traffic if in transparent mode and if Layer 2 bypass is enabled. NSRP packets are not passed.

The fiber Ethernet ports are standard interfaces and do not incorporate the integrated bypass feature. Automatic bypass is available for fiber ports through third-party devices.

## NIC Bypass and Cable Choices

When NIC bypass becomes active, it physically connects the pair of forwarding interfaces to each other with a crossover cable.

If you are connecting devices that support auto-MDIX (medium dependent interface crossover) to automatically switch to the proper configuration after a cable is connected, and then you can use whatever cables you want, because auto-MDIX negotiates the correct connection. However, if neither of the devices supports auto-MDIX, and then you need to take special care to choose the right cables.

Suppose two devices, one connected to one sensor port and the other connected to the other sensor port, are instead connected directly together.

- If the two devices are connected with a straight-through cable, use one straight-through cable and one crossover cable to connect the sensor to these devices. When NIC bypass starts, the resulting effect is to create one, long straight-through cable connecting the devices.
- If the two devices are connected with a cross-over cable, use two straight-through cables to connect the sensor to these two devices. When NIC bypass starts, the resulting effect is to create one, long straight-through cable connecting the devices.

## External Bypass Unit State

This state is only available when the sensor is in transparent mode. It behaves the same as normal state, except that NSRP packets are passed even if Layer 2 bypass is not enabled.

**NOTE:** The **External Bypass Unit** setting is global. Selecting it for any interface pair enables it for all interface pairs on the sensor. If enabled for one interface pair, all interface pairs pass NSRP packets regardless of their individual settings.

The external bypass unit state appears only in the **after system unavailability** list of the ACM. However, selecting it there enables it globally for all states.

## NICs Off State

During sensor operation, this state behaves the same as normal state. NSRP heartbeats are not passed unless the sensor is in transparent mode and Layer 2 bypass is enabled. The difference is this: when the sensor software becomes unavailable because of graceful shutdown or unexpected failure, the NICs turn off and no longer appear live to other devices on the network.

This setting is not global. It must be selected for each interface pair and in each mode (**after system unavailability** and **after graceful shutdown**).

### *Peer Port Modulation*

After peer port modulation (PPM) is enabled, the sensor deactivates all the interfaces in that virtual router if the link goes down for any of the interfaces in a virtual router. All devices connected to the virtual router will detect a port failure and must be configured to take appropriate action.

You cannot enable NIC bypass and PPM on the same sensor. On the IDP 75, 250, 800, and 8200 sensors:

- PPM works on both copper and fiber interfaces.
- PPM works by turning off appropriate interfaces. Because of this, interface speeds can be set to auto on the sensor and on attached switches.

## Management Ports

These ports are provided on all IDP sensors.

### Console Serial Port

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

### Management Port

The management port provides access to the ACM to the sensor through 10/100/1000 Mbps Ethernet. The ACM is accessed from the management port and entering the correct URL in a browser window (https://*SensorIPAddress*).

**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.

## Hard Drives and USB Ports

Table 5 describes the hard drives and USB ports available on each sensor.

**Table 5: IDP Sensor Drives**

| IDP Sensor | Drives |
|---|---|
| 75, 250 | ■ One USB port<br>■ One internal hard drive |
| 800, 8200 | ■ One USB port<br>■ Two externally accessible, hot-swappable, RAID-1 mirrored hard drives |

## Power Supplies

Table 6 describes the types of power supplies available on each sensor.

**Table 6: IDP Sensor Power Supplies**

| IDP Sensor | Power Supplies |
|---|---|
| 75 | One fixed power supply. |
| 250 | One removable power supply. |
| 800, 8200 | Two removable hot-swappable power supplies.<br>Both sensors are shipped with the AC power supply.<br>The DC power supplies are optional as FRUs. |

## IDP Sensor LEDs

This section describes the LEDs for the following IDP sensor components:

- System status
- Management and high availability ports
- Traffic ports
- Hard drives
- Power supply (back panel)

### *System Status LEDs*

The IDP 75, 250, 800, and 8200 sensors each have three system status lights on the front panel to indicate power, hard drive activity, and overheating. See Table 7.

**Table 7: Front Panel System Status LEDs**

| Color | Function | LED Action Status Description |
|---|---|---|
| Green | Power | ■ Stays on when powered on.<br>■ Stays off when powered off. |
| Yellow | Hard drive activity | Flickers with activity. |
| Red | Fault | ■ Blinks slowly when a fan fails.<br>■ Blinks quickly when system is overheated.<br>■ Stays on when the power supply fails.<br>■ Stays off when the system is functioning at a normal temperature. |

### *Management and High Availability Port LEDs*

Management and high availability (HA) ports each have two LEDs—LINK and TX/RX (Figure 8). Management ports are on all sensors. HA ports are available on the IDP 250, 800, and 8200 sensors only. Table 8 describes the LEDs for management and HA ports

**Figure 8: LEDs for Management and HA Ports**

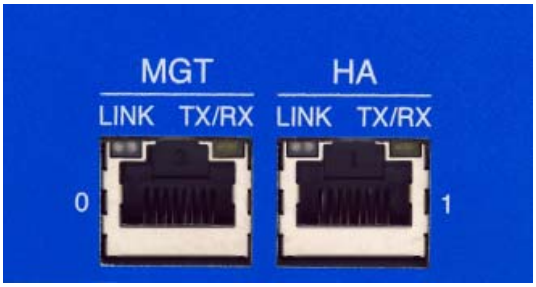



**Table 8: IDP Sensor Management and High Availability Port LED**

| Port LED | Description | Status |
|---|---|---|
| LINK | Port connection/ activity indicator. | Blinks amber to indicate activity on the port. |
| TX/RX | Speed indicator. | ■ Stays off for 10 Mbps.<br>■ Glows green for 100 Mbps.<br>■ Glows amber for 1000 Mbps. |

## *Traffic Port LEDs*

The IDP 75, 250, 800, and 8200 sensors each have two traffic status LEDs on each traffic port.

**Table 9: IDP Sensor Traffic Port LEDs**

| Indicator | Location | Color/Status | Speed/Description |
|---|---|---|---|
| Link Activity | Left LED | Green | ■ Stays on when there is a link.<br>■ Stays off when there is no link.<br>■ Blinks when there is activity. |
| Link Speed | Right LED | None | 10 Mbps |
| | | Green | 100 Mbps |
| | | Yellow | 1 Gbps |
| | | Orange | 10 Gbps |

## *Hard Drive LEDs on Front Panel*

The front panel of the sensors provide access to hard disk drives for 800 and 8200 sensors only. Table 10 shows the hard drive LED definitions for the 800 and the 8200 sensors.

**Table 10: Hard Drive LED Definitions**

| Front Panel LED | Description |
|---|---|
| Hard drive failure (800 and 8200 only) | The left LED on the hard drive. The LED is off if the hard drive is functioning normally. The LED is red if the hard drive has failed. In addition, the system emits a high-pitch noise if a hard drive has failed.<br>The LED flashes red if the drive is being rebuilt. Do not turn the power off, unplug the unit, or remove either drive while the drive is being rebuilt. |
| Hard drive activity<br>(800 and 8200 only) | The right LED on the hard drive. The LED flashes green to indicate hard drive activity. |

## *Power Supply LEDs on Back Panel*

The back panel of the sensors provide access to power supplies on the 800 and 8200 sensors only. Table 11 shows the power supply LED definitions for the 800 and the 8200 sensors.

**Table 11: Power Supply LED Definitions**

| Back Panel LED | Description |
|---|---|
| Power Supply Status (800 and 8200 only) | The LED is located on the power supply above the plug socket. It glows amber to indicate that the power supply is receiving power. It glows green to indicate that the power supply is powering the unit. If a power supply has failed, or is not receiving power, the system emits a high-pitched whine. |

Chapter 3

# Installing the Sensor

This chapter describes how to install the IDP sensor in an equipment rack. This chapter has the following sections:



## General Installation Guidelines

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

**WARNING:** Never assume that the power supply is disconnected from a power source. *Always* check first.

**CAUTION:** Room temperature might not be sufficient to keep equipment at acceptable temperatures without an additional circulation system. Ensure that the room in which you operate the IDP sensor has adequate air circulation.

- Do not work alone if potentially hazardous conditions exist.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.

**NOTE:** Although you can place the IDP sensor on a desktop for operation, we do not recommend deploying it in this manner.

**CAUTION:** To prevent abuse and intrusion by unauthorized personnel, it is extremely important to install the IDP sensor in a locked-room environment.

## Rack Mounting the IDP Sensor

The location of the sensor and the layout of your equipment rack or wiring room are crucial for proper system operation.

Use the following guidelines while configuring your equipment rack.

- Enclosed racks must have adequate ventilation. An enclosed rack should have louvered sides and a fan to provide cooling air.
- When mounting a chassis in an open rack, ensure that the rack frame does not block the intake or exhaust ports. If you install a chassis on slides, check the position of the chassis when it is seated all the way into the rack.
- In an enclosed rack with a ventilation fan in the top, equipment higher in the rack can draw heat from the lower devices. Always provide adequate ventilation for equipment at the bottom of the rack.
- Baffles can isolate exhaust air from intake air. The best placement of the baffles depends on the airflow patterns in the rack.

The IDP 75 sensor occupies one rack unit (RU) in an equipment rack. One RU is 1.75 inches (44.45 mm) high. The IDP 250, IDP 800 (copper ports), and IDP 8200 sensors occupy two rack units in an equipment rack.

### *Required Tools*

Rack mounting requires the following tools:

- Flathead screwdriver
- Number 2 Phillips-head screwdriver
- Rack-compatible screws
- Rack-mounting brackets (included). Each device comes with the following brackets:
    - Two side-mounted rails for mounting to the front and back of the rack
    - Four midmount brackets for midmounting 2 RU devices
    - Two midmount brackets for midmounting 1 RU devices

### *Mounting Using Device Rack Rails*

To mount the sensor using the rails in a device rack:

1. Use a flathead screwdriver to 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 9.

**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. Slide the chassis into a set of rails.

**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.

## *Mounting Using Midmount Brackets*

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

1. Use a flathead screwdriver to attach one rack-mounting bracket to each side of the chassis with the bracket screws. See Figure 10 and Figure 11.

**Figure 10: 2 RU Device Midmount Bracket**

**Figure 11: 1 RU Device (IDP 75) 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 devices only) Attach the other two midmount brackets to the chassis and the back of the rack to hold the device securely in place.

## Connecting Power

**NOTE:** Power is provided to the IDP sensor using 90/264 VAC from your facility.

To connect power to your sensor:

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. (For IDP 800 and 8200 sensors only) Connect the second power cable to the receptacle on the second power supply. This step is optional for the IDP 8200 sensor.

4. (For IDP 800 and 8200 sensors only) Connect the other end of the second power cable to the electrical outlet. This step is optional for the IDP 8200 sensor.

**NOTE:** If you have two power supplies and do not connect both of them, the PS FAIL warning light illuminates and the sensor emits a warning tone when it is turned on.

Chapter 4

# Configuring the IDP Sensor

This chapter describes how to connect to the IDP sensor and configure the device for your network. After you have configured the sensor, you need to connect the device in your network.

This chapter has the following sections:



## Initial Configuration Options

When you first configure your sensor, you can choose a simple configuration that sets options to the most commonly used settings, or you can do an advanced configuration that allows you to choose each option individually.

### *Simple Configuration*

A simple configuration can be done using the console serial port and the EasyConfig utility, or through the management port and the QuickStart utility.

#### Simple Configuration Settings

A simple configuration lets you specify the following settings:

- Sensor mode (inline transparent or passive sniffer)
- IP address
- Netmask
- Default gateway
- Time and time zone

### Simple Configuration Values

A simple configuration has the following settings and values:

- Root password—abc123
- Fully qualified domain name—Blank
- High availability mode—Disabled
- RADIUS support—Disabled
- Network interfaces—Auto
- Virtual routers—
  - Sniffer mode: One virtual router created (vr0)
  - Transparent mode: One virtual router created for each pair of interfaces
- DNS—Disabled
- NTP—Disabled
- SSH on management port—Enabled
- Run ACM process on sensor startup—Enabled

### *Advanced Configuration*

If you wish to use a sensor mode other than inline transparent or passive sniffer, or if you do not want to use the default options for the other settings, you will have to use the Appliance Configuration Manager. See "ACM Advanced Configuration" on page 26.

## Connecting to the Sensor

Your sensor has two management interfaces: a console serial port and a management Ethernet port. You can use either one to set the sensor IP address and other basic configuration parameters.

The console serial port is used only for configuring and troubleshooting. After the sensor is configured, you can disconnect the console port. The management port, however, must be able to reach the NSM device server over the network. For this reason, you must give the sensor an IP address that the NSM device server can reach.

### *Using the Console Serial Port to Configure the Sensor*

Use this procedure if you want to set up your sensor in simple configuration, or if you just want to set an IP address so the sensor is reachable over the network. After the sensor's management interface settings are in place, you can reconfigure the sensor over the network.

To configure your sensor using the console serial port, do the following:

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

2. Connect the other end of the cable to the serial port of your workstation.

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 IDP sensor.

   If nothing appears in the terminal window, press Enter to display the boot messages.

5. Log into the IDP sensor as name (root) and password (abc123).

   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 sensor.

### *Using the Management Port to Configure the Sensor*

You can choose a simple or advanced configuration for the sensor using the management port.

To connect the dedicated management port:

1. Attach your Ethernet cable to the dedicated management RJ-45 port (MGT) located at the front of the chassis.

2. Connect the other end of your Ethernet cable to a switch or hub (recommended) or to a standalone computer.

Verify that the link LED on the management port is green, indicating a proper connection. (See Table 8 on page 15.)

#### Connecting Directly Using the Management Port

You can configure your sensor by directly connecting to the management port with a crossover Ethernet cable. The default IP address of the sensor is 192.168.1.1 in the Address or Location box.

To connect directly to the management port:

1. Connect your computer directly to the sensor using an Ethernet cable.

2. On a connected computer, open a Web browser. Type **https://192.168.1.1**.

**NOTE:** Because the ACM uses an SSL connection, you must type **https://** before the IP address.

3. Type the default user name (**root**) and password (**abc123**).

4. Skip to "Simple or Advanced Configuration Using the Management Port" on page 25.

### Connecting Remotely Using the Management Port

To connect to the management port remotely over the network, you must first have configured an IP address for the sensor. See "Using the Console Serial Port to Configure the Sensor" on page 22.

To connect remotely to the management port:

1. On a connected computer, open a Web browser.

2. Type the URL of the ACM wizard using the IP address you configured. For example, if you configured the IP address 10.100.200.1 on the IDP sensor, type **https://10.100.200.1** in the browser's Address or Location box.

**NOTE:** Because the ACM uses an SSL connection, you must type **https://** before the IP address.

3. Type the default user name (**root**) and password (**abc123**).

4. Go to "Simple or Advanced Configuration Using the Management Port" on page 25.

## *Simple or Advanced Configuration Using the Management Port*

The IDP sensor management port provides two different, but compatible, configuration paths. The QuickStart option lets you configure the default IDP settings quickly, while the Appliance Configuration Manager (ACM) option lets you make more advanced changes to the sensor configuration.

After you log into the Web-based tools using the management port, you are presented with two options: QuickStart and ACM. If you want to do a simple configuration, click **QuickStart** and fill out the fields based on the information in Table 12 on page 26.

If you want to do an advance configuration, click **ACM**, and then click **Start Configuration Wizard**. Fill out the fields in the wizard based on the information in Table 13 on page 26.

## QuickStart Simple Configuration

Table 12 provides the information you need for a simple configuration.

**Table 12: Information Needed for QuickStart Configuration**

| Field | Configuration Information |
|---|---|
| Device Deployment mode | QuickStart offers the two most popular deployment modes. If you want to use one of the other deployment modes, use the ACM instead.<br>■ **Sniffer**—You want the sensor to report on security events, but not take action to prevent them.<br>■ **Inline transparent**—You want traffic to flow through the sensor. In this mode, the sensor can block or drop traffic that violates security parameters. |
| Management Interface IP Address | The IP address of the sensor management interface. |
| Management Interface Netmask | The netmask for the management interface IP address. |
| Default Route | Your network's default route. |
| Timezone/ Date/ Time | The time zone, date, and time where the sensor resides. |
| Other settings | All other settings are the same as for "Simple Configuration" on page 21. |

## ACM Advanced Configuration

The ACM controls advanced configuration options, such as RADIUS, DNS, and SSH configurations.

The sections listed in Table 13 correspond to sections in the ACM wizard. To start the wizard, open ACM, then select **ACM** from the initial page.

For detailed information about ACM, see the ACM online help.

**Table 13: Information Needed for ACM Configuration**

| Section | Configuration Information |
|---|---|
| Setup | ■ IDP sensor root and admin passwords (default is abc123).<br>■ The new passwords you want to assign to the root and admin accounts.<br>■ The fully qualified domain name that you want to assign to the sensor. (Example: Sensor1.example.com) |
| Mode | ■ Deployment mode you have chosen: sniffer, router, bridge, transparent, or proxy-ARP. If the mode you wish to use is already selected, select it again to progress to the next screen. (The following modes are not available on the IDP 8200 sensor: router, bridge, and proxy.)<br>For transparent mode, specify whether to enable Layer 2 bypass.<br>■ Your need for HA. See "Planning an Installation" on page 1. More information on HA modes can be found in the *NetScreen-Security Manager Administrator's Guide*. |

**Table 13: Information Needed for ACM Configuration (continued)**

| Section | Configuration Information |
|---|---|
| Networking | ■ Speed and duplex settings for IDP sensor interfaces. (Normally, these can be set to auto-detect. With some switches, the speed and duplex settings have to be set manually.)<br>■ The VLAN interfaces you want to configure.<br>Virtual LANs are not available for transparent or sniffer mode, though security policies can apply rules based on VLAN tagging in these modes.<br>■ The virtual router information you want to configure.<br>More information on virtual routers can be found in the *NetScreen-Security Manager Administrator's Guide*.<br>■ The IP address and netmask for the management interface.<br>■ Forwarding interface information, such as, which ports will be connected to which external devices.<br>■ Routing table. |
| System | ■ Enable/configure DNS.<br>This is optional. Set if you want the sensor to be able to do DNS lookups.<br>■ Time and time zone.<br>■ Enable/configure NTP.<br>This is optional. Set if you want the IDP device to get its time information from an NTP server.<br>■ Enable/configure RADIUS support.<br>This is optional. Set if you want certain users to be authenticated using RADIUS. You can enable RADIUS authentication for CLI access, ACM access, or both.<br>■ Enable/configure SSH access.<br>This is optional. Set if you want to access the sensor using a terminal window, or if you want to be able to upload upgrade files to the sensor.<br>See the ACM online help for more information on system settings. |
| Management | ■ IP address of the primary and secondary NSM GUI servers for this sensor and a one-time password.<br>These values need to be set only if you are using the IP unreachable method of adding devices to NSM. See the *NetScreen-Security Manager Administrator's Guide*.<br>■ Enable/configure ACM access.<br>Set if you want ACM to start automatically when the sensor boots. Otherwise, you have to start ACM from the command line before you access it.<br>■ Instant Virtual Extranet (IVE) communications.<br>Select **Reset IVE OTP** if you want to generate a one-time password for IVE-IDP communications.<br>Complete information for configuring IVE-IDP communications is in the IVE documentation. |
| Done | View the current configuration and then save and apply the configuration to the IDP sensor. (The Save Only option button tells the sensor to save the configuration into a working file, but not to apply the configuration to the sensor. The Save & Apply option button tell the sensor to apply the changes.) You need to click Confirm Configuration, and then reboot the IDP sensor for the changes to take effect. |

In proxy-ARP or router mode, if you are using multiple subnets in your protected network, you must configure static routes on the IDP sensor to these subnets. Without static routes, incoming traffic to those subnets can be lost. Alternatively, you can create a static route from the IDP sensor to an internal gateway that contains inbound routes to the protected subnets. (This does not apply to the IDP 8200 sensor.)

## Connecting Forwarding Interfaces

Connect the ports on the sensor to either the protected network or the external network. See "Planning an Installation" on page 1 for the configuration you chose to implement. See "NIC Bypass and Cable Choices" on page 12 for information on using NIC bypass with transparent mode.

Inline transparent mode makes use of pairs of interfaces. On most sensors, the pairs are horizontal port pairs 0-1and 2-3 on each NIC. Traffic in inline transparent mode only flows between paired interfaces. You cannot have traffic flow from port 0 to port 2, for example, in inline transparent mode.

Other modes, such as router and proxy-ARP mode, do support non-paired interfaces.

## Verifying Traffic Flow

To verify that traffic is flowing through your sensor:

1. Make sure your sensor is connected to a live traffic feed.
2. Log onto the sensor as root using the console serial port, or open an SSH connection to the management port.
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
```

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

## Connecting the High Availability Port

After you have set up both machines in the HA cluster, connect their HA ports to each other using a crossover cable.

Chapter 5

# Adding the Sensor to NSM

This chapter describes how to add the IDP sensor to NetScreen-Security Manager (NSM) and push the Recommended policy. When you have completed the steps in this chapter, your IDP sensor will be protecting your network.

You must have NSM installed to complete the steps in this chapter. See the *NetScreen-Security Manager Installation Guide*.

This chapter has the following sections:



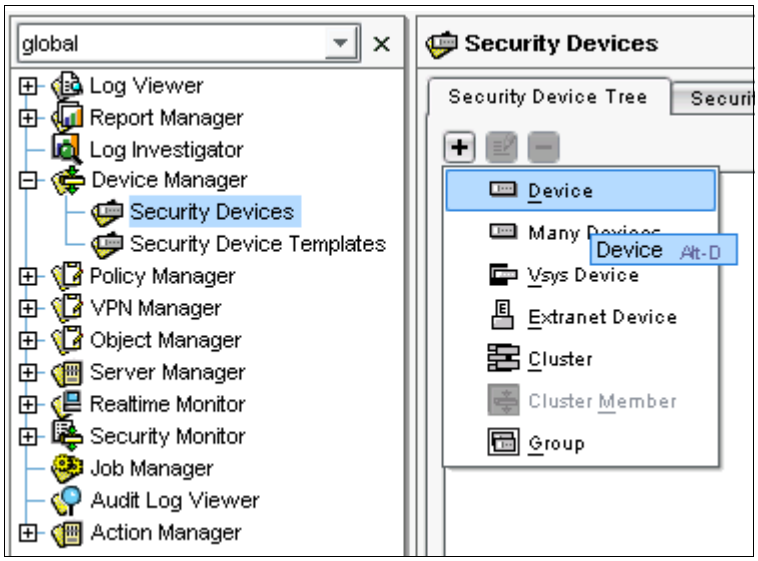
## Adding Your Sensor to NSM

This procedure assumes your sensor is installed, has a static IP address, and is reachable using SSH. If your sensor is not yet available, has a dynamic IP address, or is not reachable using SSH, see the *IDP Concepts and Examples Guide* for other procedures.

To import an IDP 75, 250, 800, or 8200 sensor with a known IP address:

1. In NSM, select **Tools > View / Update NSM Attack Database** to run the attack database wizard. This makes sure your attack database is up to date.
2. From the domain menu, select the domain in which to import the device.
3. Select **Device Manager > Security Devices** from the left navigation pane (Figure 12).

**Figure 12: Begin Add Device Procedure**

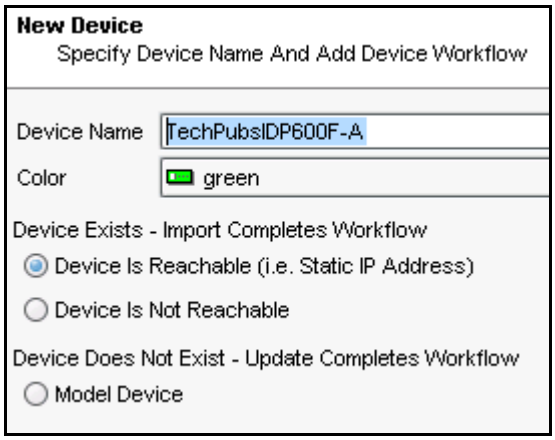



4. On the Security Devices age, click the + button and select **Device** to open the Add Device wizard (Figure 13).

   a. Type a name and select a color to represent the device in the UI.

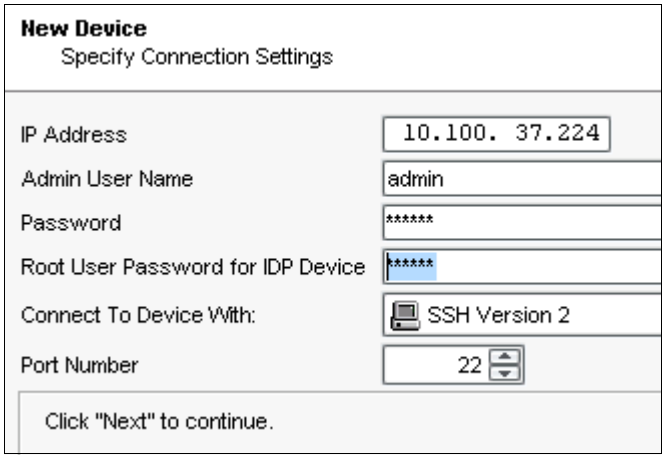
   b. Select **Device is Reachable** (default).

**Figure 13: Add Device Wizard - Device Name**




5. Click **Next** to display the Specify Connection Settings dialog box (Figure 14).

**Figure 14: Add Device Wizard - Connection Settings**




6. Enter the following connection information:

**NOTE:** All passwords handled by NetScreen-Security Manager are case-sensitive.

   a. Enter the IP address of the sensor.

   b. Enter **admin** in the Admin User Name box.

   c. Enter the password for the admin user name. The default password is abc123.

   d. Enter the password for the device root user. The default password 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 15). After a moment, the wizard displays the SSH key fingerprint information.

**Figure 15: Add Device Wizard - Verification Settings**

7. Verify the SSH key fingerprint to prevent man-in-the-middle attacks:

   a. Connect a PC or terminal to the IDP sensor using the console serial port.

   b. Log in as root.

   c. Type **cd /etc/ssh** and press Enter.

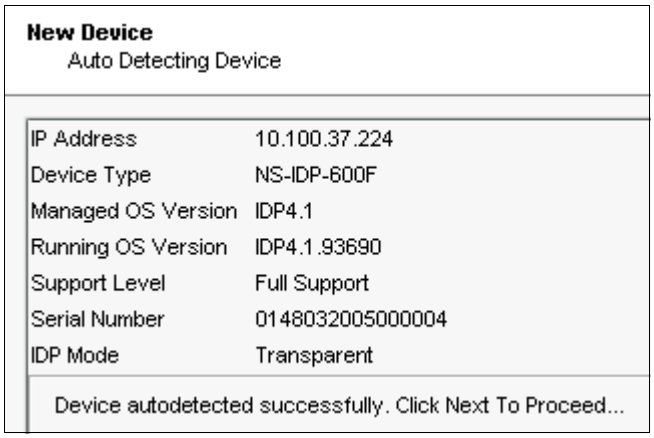
   d. Type **ssh-keygen -l -f ssh_host_dsa_key** and press Enter.

   You see something similar to this:

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

8. After you have verified the key, click **Next** to display device information retrievable by NSM (Figure 16). This takes a moment.

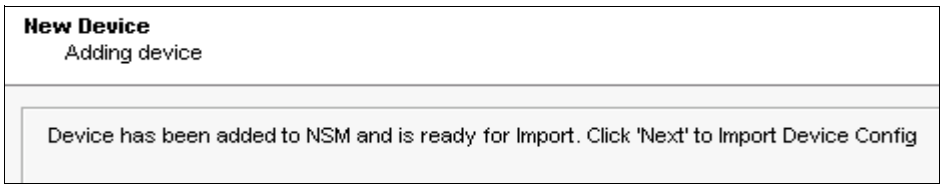
**Figure 16: Add Device Wizard - Retrieved Settings**




9. Verify that the device type, OS version, device serial number, and device mode are correct.

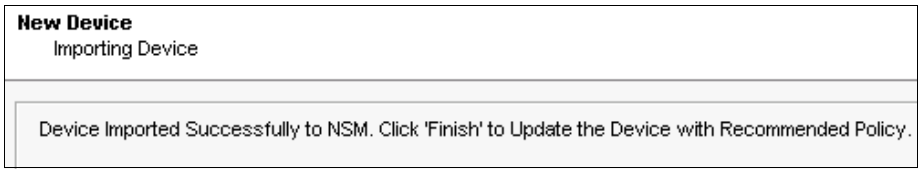
10. Click **Next** to add the sensor to NSM as a managed device. (See Figure 17.)

**Figure 17: Add Device Wizard - Adding the Device**




11. Click **Next** to have NSM import settings already present on the sensor. (See Figure 18.)

**Figure 18: Add Device Wizard - Importing the Device**



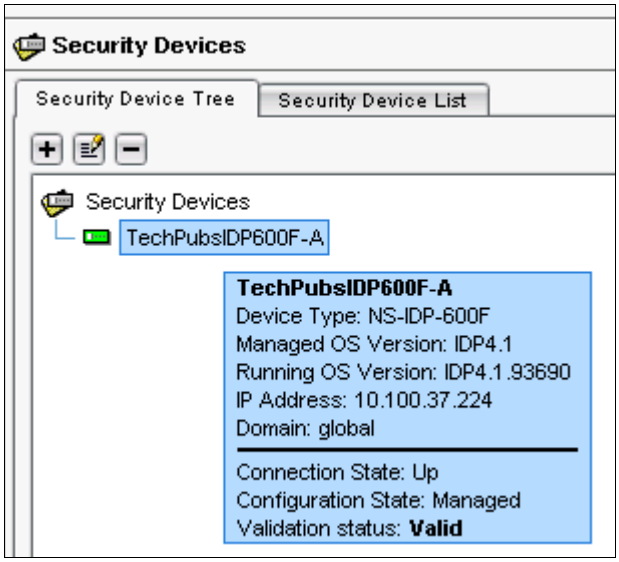

12. Click **Finish** to update the sensor with the Juniper Networks Recommended policy.

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

## Checking the Status of Your Sensor

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 19).

**Figure 19: Viewing Device Status**




NSM is now managing your sensor. See the *IDP Concepts & Examples Guide* for more information on managing your sensor.

Chapter 6

# Updating Software on the Sensor

This chapter describes how to update the software on an IDP sensor. It has the following sections:



## Updating IDP Sensor Software Using NSM Firmware Manager

You can use NSM to upgrade your IDP sensors. First, you must load a new sensor image to NSM. Then, use NSM to load the new image onto your sensors.

### *Loading a Sensor Image into NSM*

To make the sensor software available to NSM:

1. Download firmware image files from Juniper Networks onto the computer running the NSM GUI.
2. In NSM, select **Device Manager > Security Devices** from the left navigation pane.
3. From the menu bar, select **Tools > Firmware Manager**. The Firmware Manager dialog box appears.
4. Click the **+** button to open the Open dialog box.
5. Select the image file on the computer running NSM and click **Open**. The image file appears in the Firmware Manager dialog box, displaying the image name, version, and applicable devices.
6. Click **OK**.

### *Upgrading Sensor Software*

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

To upgrade the sensor using NSM:

1. From the menu bar, select **Devices > Firmware > Change Device Firmware** to open the Change Device Firmware dialog box.
2. Select the devices whose firmware you want to upgrade.
3. Select the firmware you want installed on the device in the Select Target Firmware Version box.
4. Click **Next** to display the device(s) and firmware that NetScreen-Security Manager is to install in the Firmware Update Availability dialog box.
5. Select **Automate ADM Transformation** to automatically update the Abstract Data Model (ADM) for the device after NSM installs the firmware. If you clear the Automate ADM Transformation checkbox, the firmware is installed onto the device, but you cannot manage the device from NSM until the device ADM is updated.
6. Click **Finish** to display upgrade status in the Job Information dialog box.
7. When the upgrade finishes, click **Close** to exit the Job Information dialog box.

## Updating IDP Sensor Software Without NSM

New versions of the IDP sensor software may be made available online or on a CD-ROM.

To install the new software:

1. Verify that you have SSH enabled for the Management Port (eth0).
   To enable SSH, access ACM by typing https://*sensorIPaddress* in the Address or Location box of the Web browser. Then select **Modify SSH Access** from the ACM home page and follow the prompts.

   access ACM by typing https://*sensorIPaddress* in the Address or Location box of the Web browser.
2. Download the sensor software from Juniper Networks and copy the file to the /tmp directory of the sensor.
3. Unplug the HA port cable, if one is attached.
4. Log into the IDP sensor as root using the console serial port.
5. Change to the /tmp directory.
6. Type **sh sensor_<version>.sh** and press Enter.

   The sensor update script runs.

7. Reboot the device when the script is finished.
8. Type **`reboot`** and press Enter.
9. Reconnect the HA cable after upgrading all of the sensors in the cluster.
10. In NSM, right-click the sensor in Device Manager, and then select **Adjust OS Version**.

## Reimaging the IDP Sensor

Each IDP sensor comes with software preinstalled. However, if you need to reload the software onto your sensor, you can use the USB stick that was shipped with the sensor. This process is known as *imaging*.

**NOTE:** You will need to reinstall the license when reimaging the IDP sensor. Contact JTAC for information on how to obtain your license information. Go to Requesting Technical Support on page xii for information on how to contact JTAC.

To reimage the IDP sensor:

1. Connect a PC to the console serial port of the device, using the serial cable provided with the IDP sensor.
2. Power off the IDP sensor.
3. Insert the “Restore Media” USB stick into the USB flash drive on the front of the sensor.
4. Power on the IDP sensor.

   The sensor boots from the USB stick and runs the reimaging process. Follow any prompts on the serial console. When instructed to do so at the end of the imaging process, reboot or power-cycle the IDP sensor.
5. When the process is complete, configure the IDP sensor according to the instructions in Chapter 5, “Configuring the IDP Sensor,” on page 21.

Chapter 7

# Servicing the Device

This chapter describes the service and maintenance of various components in your IDP sensors. It has the following sections:



## Replacing a Power Supply (IDP 800, and 8200 Only)

The power supplies on the IDP 75 and 250 sensors are in a fixed configuration so you cannot replace them. The IDP 800 sensor has two hot swappable power supplies while the IDP 8200 sensor has three.

If a device has two replaceable power supplies, you can hot swap one while the device is running. Contact Juniper Networks if you want to purchase a spare power supply.

### *Remove a Power Supply*

To remove a power supply:

1. Go to the back of the device and locate the power supply you want to remove.
2. Locate the horizontal handle and the red lever in the upper left corner of the power supply.
3. Lift the handle and push the lever to the right to unlatch the power supply.
4. With the lever pushed to the right, pull on the handle firmly to dislodge the power supply from its seating.
5. Let go of the lever and slide out the power supply from the handle.
6. Let go of the handle and use both hands to slide the power supply the rest of the way out.

### *Install a Power Supply*

You must have a power supply bay available before you can install a power supply.

To install a power supply:

1. Take the new power supply to the back of the device.
2. Hold the power supply with both hands with the red handle on the left side of the power supply,
3. Align the power supply with the empty bay and slide the power supply into the bay.
4. Push firmly until you see and hear the red lever snap into place.

   If the other power supply is on and powering the sensor, the sensor emits a high-pitched whine and the power supply LED turns on.
5. Connect a power cord to the new power supply.
6. Attach the other end of the power cord to the power source.

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

## Replacing a Hard Drive (IDP 800 and 8200 Only)

The IDP 800 and 8200 sensors come with two mirrored hard drives. Both drives are hot-swappable on failure. If one fails, it may be replaced without interrupting the function of the sensor. Contact Juniper Networks if you want to purchase a spare hard drive.

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

**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.**

### *Remove a Hard Drive*

SCSI hard drives are accessible from the front panel of the sensor.

**NOTE:** We recommend replacing a hard drive only when the sensor is powered on.

To remove a hard drive:

1. On the front of the device identify the hard drive you want to remove.
2. Locate the blue release latch on the right side of the drive. (See Figure 20.)

**Figure 20: Hard Drive Latch in Closed Position**


3. Press and hold down the latch to release the handle, and then pull the handle open.
4. Use one hand to hold the drive from underneath and the other hand to remove the drive completely from the bay.

## *Install a Hard Drive*

To install a hard drive:

1. Unclip the latch on the right side of the handle.
2. Open the handle to its fully extended position.
3. Begin to slide the drive into the bay.
4. Gently slide the drive the rest of the way into the bay and snap it into place.
5. Close the drive handle up until the latch clicks into place.

After a few moments, the warning noise ceases. The red failure LED on the new drive begins to flash, indicating that the hard drive is rebuilding. Then the hard drive activity LED on both drives will flash, indicating activity on both drives.

When the red failure LED stops flashing, the hard drive is rebuilt. Rebuilding the hard drive could take 30 minutes or longer.

**CAUTION:** Leave both drives in place until the hard drive array is rebuilt. Removing either drive while the hard drive array is rebuilding can damage the system.

Chapter 8

# Advanced Configuration

This chapter describes advanced configuration options and has the following sections:



## Advanced Deployment Modes

Most IDP sensors are configured in passive sniffer or transparent mode. However, the IDP 75, 250, and 800 sensors can also be configured in bridge, router, or proxy-ARP mode.

### *Bridge Mode*

Figure 21 shows a sensor that is configured in bridge mode. Table 14 lists the advantages and disadvantages of bridge mode.

**Figure 21: Bridge Mode**

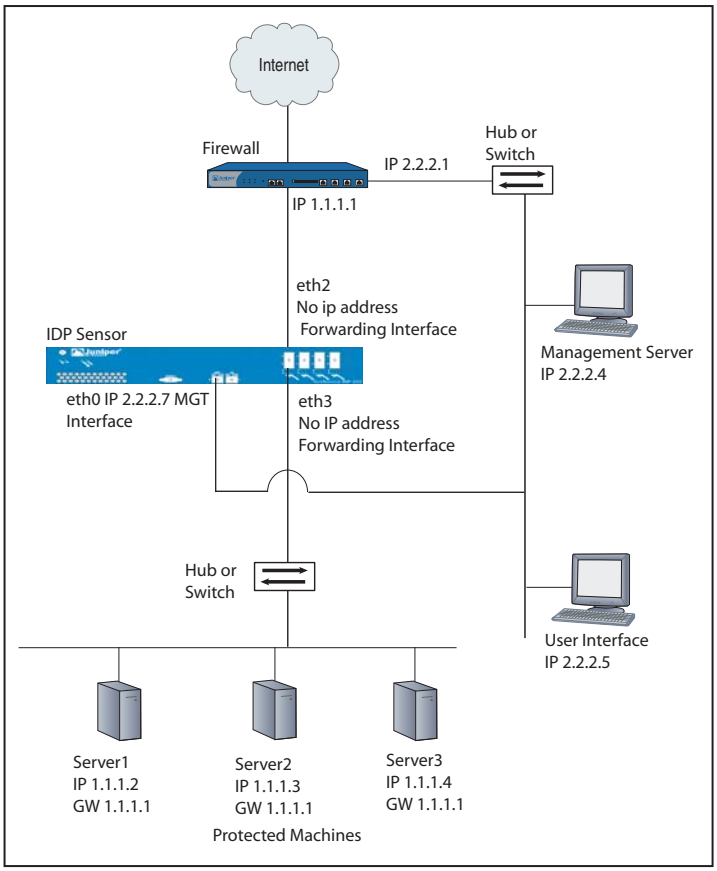



**Table 14: Advantages and Disadvantages of Bridge Mode**

| Advantages | Disadvantages |
|---|---|
| ■ Reliably responds to and prevents attacks<br>■ Simple, transparent deployment<br>■ Allows Layer 2 broadcasts<br>■ No changes to routing tables or network equipment | ■ Cannot connect IP networks with different address spaces |

## Router Mode

Figure 22 shows a sensor that is configured in bridge mode. Table 15 lists the advantages and disadvantages of bridge mode.

**Figure 22: Router Mode**

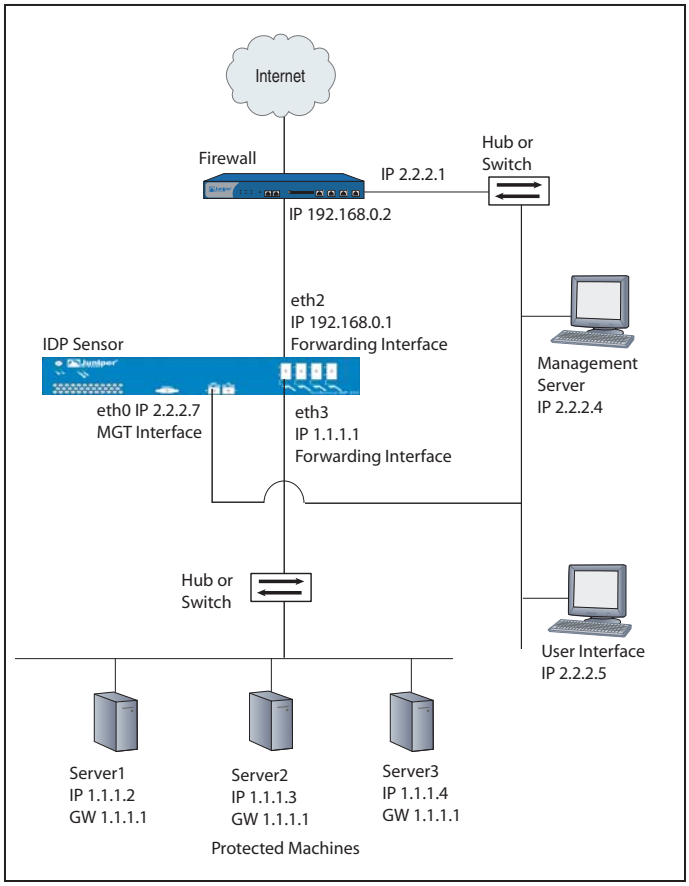



**Table 15: Advantages and Disadvantages of Router Mode**

| Advantages | Disadvantages |
|---|---|
| ■ Reliably responds to and prevents attacks | ■ Affects Layer 3 IP networks (routing tables) |
| ■ Connects IP networks with different address spaces | ■ Interfaces cannot be used in stealth mode. The sensor itself can be the target of attacks. |

### *Proxy-ARP Mode*

Figure 23 shows a sensor that is configured in bridge mode. Table 16 lists the advantages and disadvantages of bridge mode.

**Figure 23: Proxy-ARP Mode**

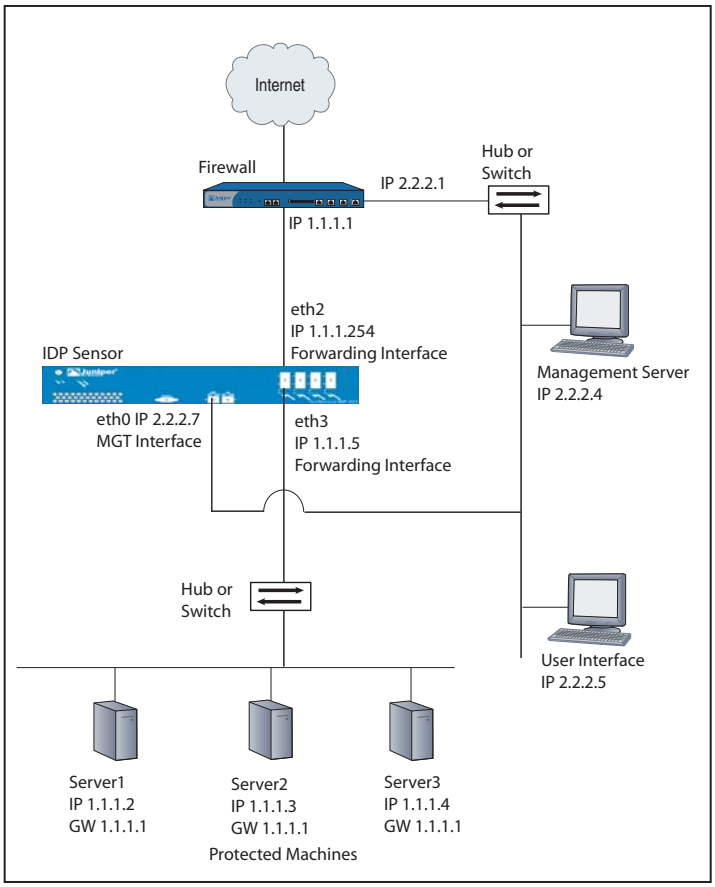



**Table 16: Advantages and Disadvantages of Proxy-ARP Mode**

| Advantages | Disadvantages |
|---|---|
| ■ Reliably responds to and prevents attacks | ■ Network nodes may need to update cached ARP entries |
| ■ Simple, transparent deployment | |

## IDP High Availability Deployment Modes

You must deploy the IDP sensors in bridge, router, transparent, or proxy-ARP mode to enable a high availability solution.For details on deployment modes and HA clusters, see the *NetScreen-Security Manager Administrator's Guide.*

Appendix A
# Specifications

This appendix provides general specifications for the IDP sensors and standards for compliance. It has the following sections:

## IDP 75 Technical Specifications

Tables 17–20 list the physical, AC power, power cord, and environmental technical specifications for the IDP 75 sensor.

**Table 17: Physical Specifications**

| Specification | Value |
|---|---|
| Height | 1 RU (1.3 inches) |
| Width | 17 inches |
| Depth | 15 inches |
| Weight | 14.5 lbs |

**Table 18: 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 | 4 A @ 110 VAC<br>2 A @ 220 VAC | |

**Table 19: Power Cord Specifications**

| Country | Specifications |
|---|---|
| United States and Canada | ■ UL-approved and CSA-certified<br>■ Flexible cord minimum spec: No. 18 (1.5 $mm^2$), Type SVT or SJT, 3-conductor<br>■ Current capacity of 10 A minimum<br>■ Earth-grounding attachment plug with NEMA 5-15P (10 A, 125 V) configuration |

**Table 20: Environmental Specifications**

| Specification | Value |
|---|---|
| Operating environment | 0 to 35° C (ambient) |
| Non-operating environment | -10° to 70° C |

## IDP 250 Technical Specifications

Tables 21–24 list the physical, AC power, power cord, and environmental technical specifications for the IDP 250 sensor.

**Table 21: Physical Specifications**

| Specification | Value |
|---|---|
| Height | 2 RU (2.9 inches) |
| Width | 17 inches |
| Depth | 20.5 inches |
| Weight | 29.5 lbs |

**Table 22: 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 | 4 A @ 110 VAC<br>2 A @ 220 VAC | |

**Table 23: Power Cord Specifications**

| Country | Specifications |
|---|---|
| United States and Canada | ■ UL-approved and CSA-certified<br>■ Flexible cord minimum spec: No. 18 (1.5 $mm^2$), Type SVT or SJT, 3-conductor<br>■ Current capacity of 10 A minimum<br>■ Earth-grounding attachment plug with NEMA 5-15P (10 A, 125 V) configuration |

**Table 24: Environmental Specifications**

| Specification | Value |
|---|---|
| Operating environment | 0 to 35° C (ambient) |
| Non-operating environment | -10° to 70° C |

## IDP 800 Technical Specifications

Tables 25–28 list the physical, AC power, power cord, and environmental technical specifications for the IDP 800 sensor.

**Table 25: Physical Specifications**

| Specification | Value |
|---|---|
| Height | 2 RU (2.9 inches) |
| Width | 17 inches |
| Depth | 20.5 inches |
| Weight | 33.5 lbs |

**Table 26: 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 | 4 A @ 110 VAC<br>2 A @ 220 VAC | |

**Table 27: Power Cord Specifications**

| Country | Specifications |
|---|---|
| United States and Canada | ■ UL-approved and CSA-certified<br>■ Flexible cord minimum spec: No. 18 (1.5 $mm^2$), Type SVT or SJT, 3-conductor<br>■ Current capacity of 10 A minimum<br>■ Earth-grounding attachment plug with NEMA 5-15P (10 A, 125 V) configuration |

**Table 28: Environmental Specifications**

| Specification | Value |
|---|---|
| Operating environment | 0 to 35$^{o}$C (ambient) |
| Non-operating environment | -10$^{o}$ to 70$^{o}$ C |

## IDP 8200 Technical Specifications

Tables 29–32 list the physical, AC power, power cord, and environmental technical specifications for the IDP 8200 sensor.

**Table 29: Physical Specifications**

| Specification | Value |
|---|---|
| Height | 2 RU (2.9 inches) |
| Width | 17 inches |
| Depth | 20.5 inches |
| Weight | 36.5 lbs |

**Table 30: 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 | 4 A @ 110 VAC<br>2 A @ 220 VAC | |

**Table 31: Power Cord Specifications**

| Country | Specifications |
|---|---|
| United States and Canada | ■ UL-approved and CSA-certified<br>■ Flexible cord minimum spec: No. 18 (1.5 $mm^2$), Type SVT or SJT, 3-conductor<br>■ Current capacity of 10 A minimum<br>■ Earth-grounding attachment plug with NEMA 5-15P (10 A, 125 V) configuration |

**Table 32: Environmental Specifications**

| Specification | Value |
|---|---|
| Operating environment | 0 to 35$^{o}$ C (ambient) |
| Non-operating environment | -10$^{o}$ to 70$^{o}$ C |

## 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
- FCC Part 15 Class A
- Industry Canada ICES-003 Class A
- VCCI Class A

## Immunity

- EN 55024, 1998

# Index