



Security Products

SSG 140 Hardware Installation and Configuration Guide

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Copyright Notice

Copyright © 2008 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

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

	About This Guide	5
	Organization	6
	Conventions	6
	Web User Interface Conventions	6
	Command Line Interface Conventions	7
	Requesting Technical Support	7
	Self-Help Online Tools and Resources	7
	Opening a Case with JTAC	8
	Feedback	8
Chapter 1	Hardware Overview	9
	Front Panel	9
	Port Descriptions	10
	Device Status LEDs	11
	Ethernet Port LEDs	12
	Reset Pinhole	12
	USB Port	12
	Back Panel	13
	Physical Interface Module Slots	13
	Power Switch	14
	AC Power Appliance Inlet	14
	Fuse Cover	14
Chapter 2	Installing and Connecting the Device	15
	Before You Begin	16
	Installing Equipment	16
	Organizing Interface Cables	18
	Connecting Power	18
	Powering the Device On and Off	18
	Connecting the Device to a Network	18
Chapter 3	Configuring the Device	21
	Accessing the Device	22
	Using a Console Connection	22
	Using the WebUI	24
	Using Telnet	24
	Default Device Settings	25
	Basic Device Configuration	26
	Admin Name and Password	26
	Administrative Access	27
	Interface IP Address	27
	Management Services	27

	Hostname and Domain Name	28
	Domain Name System Server	28
	Date and Time	28
	Default Route	29
	Bridge Group Interfaces	29
	PIM Configuration	30
	Basic Firewall Protections	30
	Verifying External Connectivity	31
	Restarting the Device	31
	Restarting the Device with the CLI Reset Command	31
	Restarting the Device with the WebUI	32
	Resetting the Device to Factory Defaults	32
	Device Serial Number	33
	unset all	33
	Reset Pinhole Button	34
Chapter 4	Servicing the Device	37
	Tools and Parts Required	37
	Replacing a PIM	38
	Removing a Blank Faceplate	38
	Removing a PIM	39
	Installing a PIM	40
	Upgrading Memory	40
	Replacing the Fuse	43
Appendix A	Specifications	45
	Physical	45
	Electrical Specifications	46
	Environmental Tolerance	46
	Certifications	47
	Connectors	48
Appendix B	Initial Configuration Wizard	51
	Index	59

About This Guide

The Juniper Networks Secure Services Gateway (SSG) 140 devices is an integrated router and firewall platform. It provides Internet Protocol Security (IPSec) virtual private network (VPN) and firewall services for small- and medium-sized companies and enterprise branch and remote offices.

NOTE: The configuration instructions and examples in this document are based on the functionality of a device running ScreenOS 6.0.0. Your device might function differently depending on the ScreenOS version you are running. For the latest device documentation, refer to the Juniper Networks Technical Publications website at www.juniper.net/techpubs/hardware. To determine which ScreenOS versions are currently available for your device, refer to the Juniper Networks Support website at <http://www.juniper.net/customers/support/>.

Organization

This guide contains the following chapters and appendixes:

Chapter 1, “Hardware Overview,” describes the chassis and components of the SSG 140 device.

Chapter 2, “Installing and Connecting the Device,” describes how to mount the SSG 140 device in a standard 19-inch equipment rack and how to connect cables and power to it.

Chapter 3, “Configuring the Device,” describes how to configure and manage the SSG 140 device and how to perform some basic configuration tasks.

Chapter 4, “Servicing the Device,” describes service and maintenance procedures for the SSG 140 device.

Appendix A, “Specifications,” provides general specifications for the SSG 140 device.

Appendix B, “Initial Configuration Wizard,” provides detailed information about using the Initial configuration Wizard (ICW) for the SSG 140 device.

Conventions

This guide uses the conventions described in the following sections:

- “Web User Interface Conventions” on page 6
- “Command Line Interface Conventions” on page 7

Web User Interface Conventions

The Web user interface (WebUI) contains a navigational path and configuration settings. To enter configuration settings, begin by clicking a menu item in the navigation tree on the left side of the screen. As you proceed, your navigation path appears at the top of the screen, with each page separated by angle brackets.

The following example shows the WebUI path and parameters for defining an address:

Policy > Policy Elements > Addresses > List > New: Enter the following, then click **OK**:

Address Name: addr_1
IP Address/Domain Name:
IP/Netmask: (select), 10.2.2.5/32
Zone: Untrust

To open online Help for configuration settings, click the question mark (?) in the upper left of the screen.

The navigation tree also provides a Help > Config Guide configuration page to help you configure security policies and Internet Protocol Security (IPSec). Select an

option from the list and follow the instructions on the page. Click the ? character in the upper left for Online Help on the Config Guide.

Command Line Interface Conventions

The following conventions are used to present the syntax of command line interface (CLI) commands in text and examples.

In text, commands are in **boldface** type and variables are in *italic* type.

In examples:

- Variables are in *italic* type.
- Anything inside square brackets [] is optional.
- Anything inside braces { } is required.
- If there is more than one choice, each choice is separated by a pipe (|). For example, the following command means “set the management options for the ethernet1, the ethernet2, or the ethernet3 interface”:

```
set interface { ethernet1 | ethernet2 | ethernet3 } manage
```

NOTE: When entering a keyword, you only have to type enough letters to identify the word uniquely. For example, typing **set adm u ang j12fmt54** is enough to enter the command **set admin user angel j12fmt54**. Although you can use this shortcut when entering commands, all the commands documented here are presented in their entirety.

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings—<http://www.juniper.net/customers/support/>
- 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/>.

Feedback

If you find any errors or omissions in this document, contact Juniper Networks at techpubs-comments@juniper.net.

Chapter 1

Hardware Overview

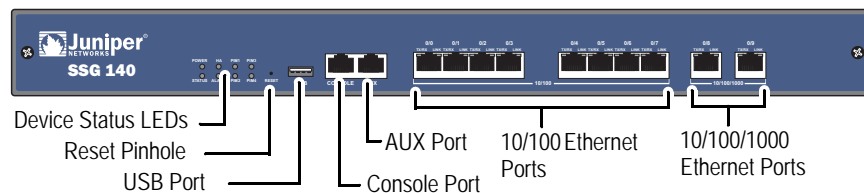
This chapter provides detailed descriptions of the SSG 140 device and its components. It contains the following sections:

- “Front Panel” on page 9
- “Back Panel” on page 13

Front Panel

Figure 1 shows the front panel of the SSG 140 device.

Figure 1: SSG 140 Front Panel



The following sections describe the elements on the front panel of the SSG 140 device:

- “Port Descriptions” on page 10
- “Device Status LEDs” on page 11
- “Ethernet Port LEDs” on page 12
- “Reset Pinhole” on page 12
- “USB Port” on page 12

Port Descriptions

Table 1 describes the function, connector type, and speed/protocol (if applicable) of the ports on the front panel of the SSG 140 device.

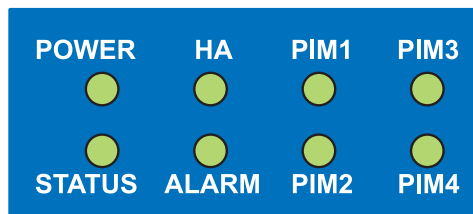
Table 1: SSG 140 Ports

Item	Description	Connector	Speed/Protocol
Ethernet 0/0 to 0/7 Ports	Enables ethernet connections to workstations or a LAN connection through a switch or hub. These connections also allow you to manage the device through a Telnet session or the WebUI. When configuring one of the ports, reference the interface name that corresponds to the location of the port. From left to right on the front panel, the interface names for the ports are ethernet0/0 through ethernet0/9 . For the default zone bindings for each Ethernet port, see “Default Device Settings” on page 25.	RJ-45	10/100 Mbps Ethernet Autosensing duplex and auto MDI/MDIX
Ethernet 0/8 to 0/9 Ports	Enables ethernet connections to workstations or a LAN connection through a switch or hub. These connections also allow you to manage the device through a Telnet session or the WebUI. When configuring one of the ports, reference the interface name that corresponds to the location of the port. From left to right on the front panel, the interface names for the ports are ethernet0/0 through ethernet0/9 . For the default zone bindings for each Ethernet port, see “Default Device Settings” on page 25.	RJ-45	10/100/1000 Mbps Ethernet Autosensing duplex and auto MDI/MDIX
USB Port	Enables a 1.1 USB connection with the device. See “USB Port” on page 12 for more information.	-	12M (full speed) or 1.5M (low speed)
Console Port	The console port is an RJ-45 serial data terminal equipment (DTE) port that can be used for either local or remote administration. For local administration, connect the port to a terminal with an RJ-45-to-DB-9 (female-to-male) straight-through serial cable. For remote administration, connect the port to a workstation with an RJ-45-to-DB-9 (female-to-male) serial cable with a null modem adapter. See “Connectors” on page 48 for the RJ-45 connector pinouts.	RJ-45	9600 bps/RS-232C serial
AUX Port	The auxiliary (AUX) port is an RJ-45 serial port wired as a DTE that you can connect to a modem to allow remote administration. We do not recommend using this port for regular remote administration. The AUX port is typically assigned to be the backup serial interface. The baud rate is adjustable from 9600 bps to 115200 bps and requires hardware flow control. See “Connectors” on page 48 for the RJ-45 connector pinouts.	RJ-45	9600 bps — 115 Kbps/RS-232C serial

Device Status LEDs

The device LEDs show information about current device status. Figure 2 shows the position of each LED on the front of the SSG 140 device.

Figure 2: Device Status LEDs



When the device powers up, the POWER LED changes from off to green and the STATUS LED changes from off to blinking green. Startup takes approximately one minute to complete. If you want to turn the device off and on again, we recommend you wait a few seconds between shutting it down and powering it back up. Table 2 lists the name, color, status, and description of each device status LED.

Table 2: Device Status LED Descriptions

Name	Color	Status	Description
POWER	Green	On steadily	Power is functioning correctly.
		Off	Device is not receiving power.
STATUS	Green	Off	Device is powered off or is starting up.
		Blinking	Normal operation.
ALARM	Red	On steadily	Critical alarm: <ul style="list-style-type: none"> ■ Failure of hardware component or software module. ■ Firewall attacks detected.
			Amber
	Off	No alarms.	
HA (High Availability)	Green	On steadily	Unit is the primary (master) device.
		Amber	Unit is the secondary (backup) device.
	Off	High availability not enabled.	
PIM (1-4)	Green	On steadily	PIM is ready for activity.
		Blinking	Traffic is present.
		Off	PIM is not present or is installed incorrectly.

Ethernet Port LEDs

The Ethernet LEDs show the status of each Ethernet port. Figure 3 shows the location of the LEDs on each Ethernet port.

Figure 3: Ethernet Port LEDs

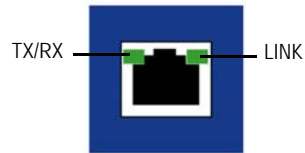


Table 3 describes the Ethernet port LEDs.

Table 3: Ethernet Port LEDs

Name	Function	Color	State	Description
LINK	Link	Green	On steadily	Port is online.
			Off	Port is offline.
TX/RX	Activity	Green	Blinking	Port is receiving data.
			Off	Port might be on, but it is not receiving data.

Reset Pinhole

The reset pinhole is a button that resets the device to its original default settings. To use this button, insert a stiff wire (such as a straightened paper clip) into the pinhole. See “Resetting the Device to Factory Defaults” on page 32 for more information.



WARNING: Because resetting the device restores it to the original default configuration, any new configuration settings are lost, and the firewall and all VPN services become inoperative. We recommend that you save the device configuration before resetting the device with the reset pinhole.

USB Port

The USB port on the front panel of an SSG 140 device accepts a universal serial bus (USB) storage device.

The USB ports let you transfer data such as device configurations, image keys, and ScreenOS software between a USB storage device and the internal flash storage of the security device. The USB ports support USB 1.1 and USB 2.0 specifications.

You can also log messages to a USB storage device. For more information about logging, refer to the *Administration* volume of the *Concepts and Examples ScreenOS Reference Guide*.

To transfer data between a USB storage device and an SSG 140 device:

1. Connect the USB storage device to either the upper or lower USB port on the security device.

2. Save the files from the USB storage device to the internal flash storage on the device with the **save {software | config | image-key} from usb filename to flash** command.
3. Stop the USB port with the **exec usb-device stop** command before removing the USB storage device.



CAUTION: Always execute the **exec usb-device stop** command before disconnecting a USB storage device. Disconnecting a USB device without executing the **stop** command may cause the device to restart.

4. Remove the USB storage device.

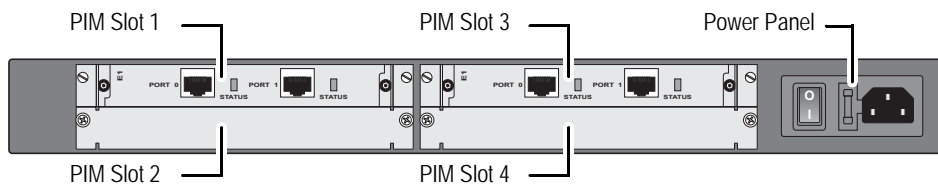
If you want to delete a file from the USB storage device, use the **delete file usb:/filename** command.

If you want to view the saved file information about the USB storage device and internal flash storage, use the **get file** command.

Back Panel

The back panel of the SSG 140 device contains four physical Interface Modules (PIM) slots and the power panel.

Figure 4: Back Panel of an SSG 140 Device



The following sections describe the elements on the back panel of the SSG 140 device:

- “Physical Interface Module Slots” on page 13
- “Power Switch” on page 14
- “AC Power Appliance Inlet” on page 14
- “Fuse Cover” on page 14

Physical Interface Module Slots

Physical interface modules (PIMs) let you add Ethernet and WAN interfaces to your SSG 140 device. For information about installing and removing PIMs, see “Replacing a PIM” on page 38. For more information about PIMs, refer to the *PIM and Mini-PIM Installation and Configuration Guide*.

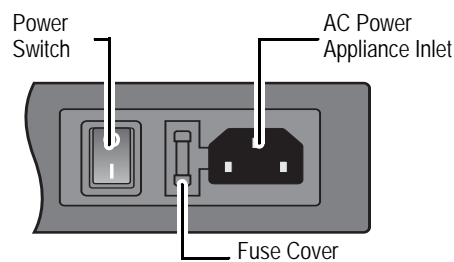


CAUTION: PIMs are not hot-swappable. Always switch off the device before inserting or removing PIMs.

Power Switch

The power switch is located on the right side of the back panel, as shown in Figure 5. You use the power switch to power the SSG 140 device on and off. When you power on the device, ScreenOS starts up as the power supply completes its startup sequence.

Figure 5: Power Switch, AC Power Appliance Inlet, and Fuse Cover



AC Power Appliance Inlet

The AC power appliance inlet is located on the right side of the back panel, as shown in Figure 5. You use the AC power appliance inlet to connect the SSG 140 device to an AC power source (90-264 VAC 50-60 Hz) using the supplied AC power cord.

Fuse Cover

The fuse cover is located on the right side of the back panel, as shown in Figure 5. To change the fuse, see “Replacing the Fuse” on page 43.

Chapter 2

Installing and Connecting the Device

This chapter describes how to install an SSG 140 device in a standard 19-inch equipment rack and how to connect cables and power to the device. Topics in this chapter include:

- “Before You Begin” on page 16
- “Installing Equipment” on page 16
- “Organizing Interface Cables” on page 18
- “Connecting Power” on page 18
- “Powering the Device On and Off” on page 18
- “Connecting the Device to a Network” on page 18

NOTE: For safety warnings and instructions, refer to the *Juniper Networks Security Products Safety Guide*. When working on any equipment, be aware of the hazards involved with electrical circuitry, and follow standard practices for preventing accidents.

Before You Begin

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



CAUTION: To prevent abuse and intrusion by unauthorized personnel, install the SSG 140 device in a secure environment.

Observe the following precautions to help 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).
- Allow 3 feet (1 meter) of clear space to the front and back of the device.
- Do not place the device in an equipment rack frame that blocks the air vents on the sides of the chassis. 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.

Installing Equipment

You can mount the SSG 140 device into a standard 19-inch equipment rack. You can center- or front-mount the device in a rack. Rack-mounting brackets are supplied with the device.

NOTE: If you are installing multiple devices in one rack, install the lowest one first and proceed upward in the rack.

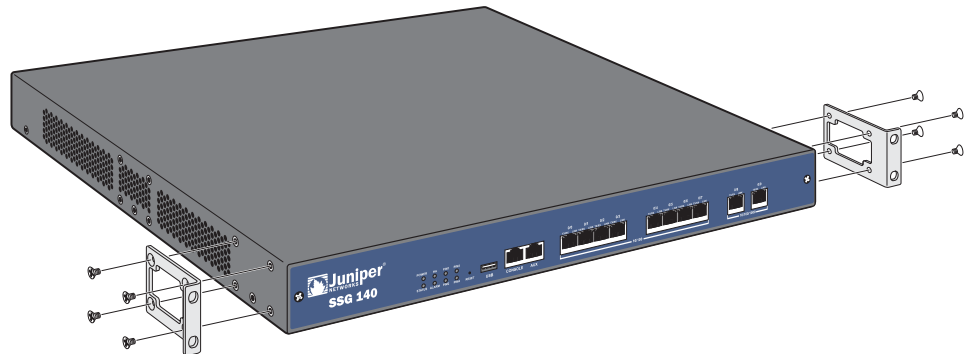
You need the following items to mount the SSG 140 device:

- Mounting brackets (provided)
- Number-2 phillips screwdriver (not provided)
- Four screws compatible with the equipment rack (not provided)

To install an SSG 140 device into a rack:

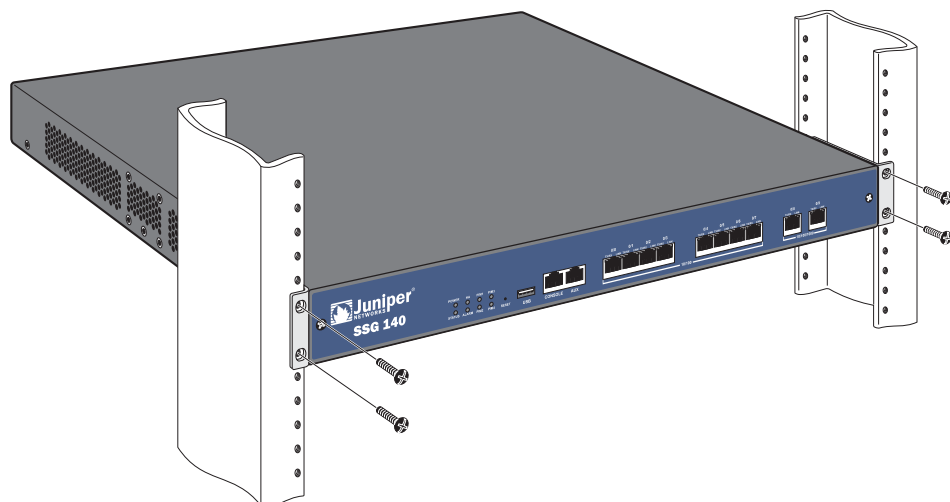
1. Attach the mounting brackets to each side of the chassis as shown in Figure 6. For front mounting, use the holes nearest the front of the device. For center-mounting, use the holes nearest the center of each side of the device.

Figure 6: Attaching Rack Mount Brackets (Front-Mount Shown, Center-Mount Similar)



2. Grasp the sides of the device, lift the device, then position it in the rack. When correctly positioned, the device sits level in the equipment rack.
3. Align the bottom hole in each mounting bracket with a hole in each rack rail, making sure the chassis is level.
4. Install a mounting screw into each of the two aligned holes. Use a number-2 phillips screwdriver to tighten the screws.

Figure 7: Rack Installation (Front-Mount Shown, Center-Mount Similar)



5. Install the remaining screws in each mounting bracket.
6. Verify that the mounting screws on one side of the rack are aligned with the mounting screws on the opposite side and that the device is level.

Organizing Interface Cables

Arrange network cables as follows to prevent them from dislodging or developing stress points:

- Secure cables so that they are not supporting their own weight as they hang to the floor.
- Place excess cable out of the way in neatly coiled loops.
- Use fasteners to maintain the shape of cable loops.

Connecting Power

The AC power cord shipped with the device connects the device to earth ground when plugged into an AC grounding-type power outlet. The device must be connected to earth ground during normal operation.

To connect power to the device, plug one end of the AC power cord into the AC power appliance inlet on the back panel of the device. Plug the other end into an AC power source.



CAUTION: We recommend using a surge protector for the power connection.

Powering the Device On and Off

To power on the SSG 140 device, press the AC power switch on the rear panel to the on position.

ScreenOS starts as the power supply completes its startup sequence. The POWER LED lights during startup and remains on steadily when the device is operating normally.

To power off the SSG 140 device, press the power switch to the off position.

Connecting the Device to a Network

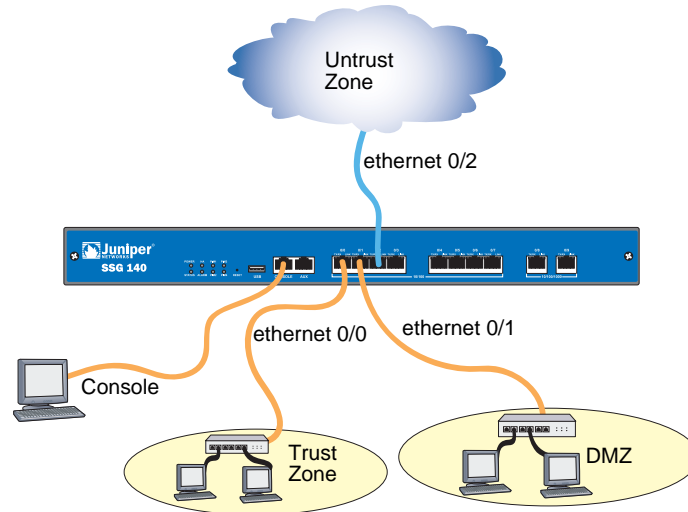
This section provides basic information about physically connecting the SSG 140 device to a network.

To connect the necessary cables as shown in Figure 8 on page 19:

1. Connect an RJ-45 cable from the port labeled **0/0** (ethernet0/0 interface) to a switch or router in the Trust security zone.
2. Connect an RJ-45 cable from the port labeled **0/1** (ethernet0/1 interface) to a switch or router in the DMZ security zone.

3. Connect an RJ-45 cable from the port labeled **0/2** (ethernet0/2 interface) to the external switch or router. The ethernet0/2 interface is prebound to the Untrust security zone.
4. Connect an RJ-45 cable from the Console port using the instructions provided in “Using a Console Connection” on page 22 for management access.

Figure 8: Basic Cabling Example



WARNING: Make sure that you do not inadvertently connect the Console, AUX, or Ethernet ports on the device to the telephone outlet.

Chapter 3

Configuring the Device

ScreenOS software is preinstalled on the SSG 140 device. When the device is powered on, it is ready to be configured. While the device has a default factory configuration that allows you to initially connect to the device, you must perform further configuration for your specific network requirements.

This chapter contains the following sections:

- “Accessing the Device” on page 22
- “Default Device Settings” on page 25
- “Basic Device Configuration” on page 26
- “PIM Configuration” on page 30
- “Basic Firewall Protections” on page 30
- “Verifying External Connectivity” on page 31
- “Restarting the Device” on page 31
- “Resetting the Device to Factory Defaults” on page 32

NOTE: After you configure the device and verify connectivity through the remote network, you must register your product at <http://www.juniper.net/customers/support/> so certain ScreenOS services, such as Deep Inspection Signature Service and Antivirus (purchased separately), can be activated on the device. After registering your product, use the WebUI to obtain the subscription for the service. For more information about registering your product and obtaining subscriptions for specific services, refer to the *Concepts & Examples ScreenOS Reference Guide* for the ScreenOS version running on the device.

Accessing the Device

You can configure and manage the SSG 140 device in several ways:

- **Console**—The Console port on the device lets you access the device through a serial cable connected to your workstation or terminal. To configure the device, you enter ScreenOS command line interface (CLI) commands on your terminal or in a terminal-emulation program on your workstation. For more information, see “Using a Console Connection” on page 22.
- **Remote Console**—You can remotely access the console interface on a security device by dialing into it. You can either dial into the v.92 modem port or into a modem connected to the AUX port. For more information, refer to the *Administration* volume of the *Concepts & Examples ScreenOS Reference Guide*.
- **WebUI**—The ScreenOS Web user interface (WebUI) is a graphical interface available through a browser. To initially use the WebUI, the workstation on which you run the browser must be on the same subnet as the device. You can also access the WebUI through a secure server using Secure Sockets Layer (SSL) with secure HTTP (HTTPS).
- **Telnet/SSH**—Telnet and SSH are applications that allow you to access devices through an IP network. To configure the device, you enter ScreenOS CLI commands in a Telnet session from your workstation. For more information, refer to the *Administration* volume of the *Concepts & Examples ScreenOS Reference Guide*.
- **Network and Security Manager**—Network and Security Manager is a Juniper Networks enterprise-level management application that enables you to control and manage Juniper Networks security devices. For instructions on how to manage your device with Network and Security Manager, refer to the *Network and Security Manager Administrator’s Guide*.

Using a Console Connection

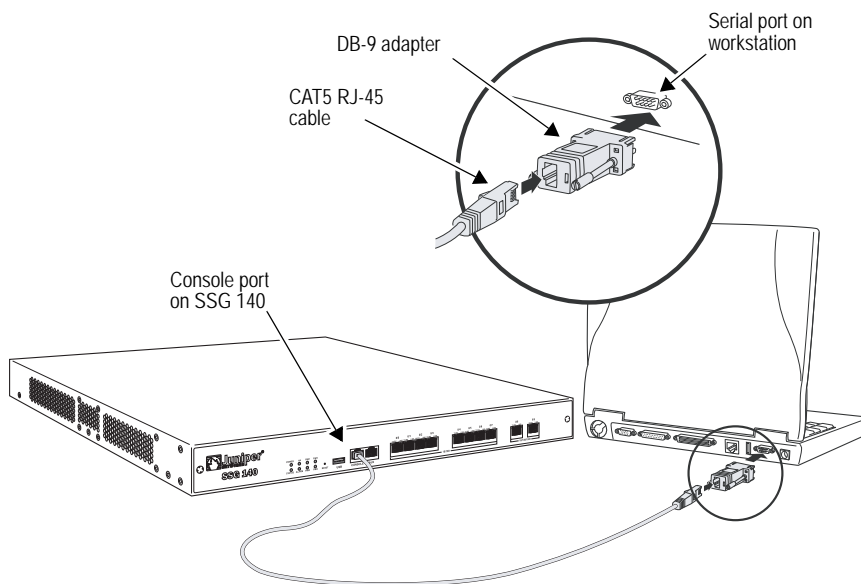
NOTE: Use a straight-through RJ-45 CAT5 cable with a male RJ-45 connector to plug into the Console port on the device.

To establish a console connection:

1. Plug the female end of the supplied DB-9 adapter into the serial port of your workstation. (Be sure that the DB-9 is inserted properly and secured.)
2. Plug one end of the RJ-45 CAT5 cable into the DB-9 adapter.

3. Plug the other end of the RJ-45 CAT5 cable into the Console port on the SSG 140. Figure 9 shows the arrangement of the cable and adapter.

Figure 9: Establishing a Console Connection



4. Launch a serial terminal-emulation program on your workstation. The required settings to launch a console session are as follows:
 - Baud rate: 9600
 - Parity: None
 - Data bits: 8
 - Stop bit: 1
 - Flow Control: None
5. If you have not yet changed the default login for the login name and password, enter **netScreen** at both the login and password prompts. (Use lowercase letters only. The login and password fields are both case-sensitive)

For information about configuring the device with CLI commands, refer to the *Concepts & Examples ScreenOS Reference Guide*.

6. (Optional) By default, the console times out and terminates automatically after 10 minutes of idle time. To remove the timeout, enter **set console timeout 0**.
7. Once the command prompt is displayed, the device is ready to be configured. See “Basic Device Configuration” on page 26 to complete the initial device configuration.

Using the WebUI

To use the WebUI, the workstation from which you are managing the device must initially be on the same subnetwork as the device. To access the device with the WebUI:

1. Connect your workstation to the port labeled 0/0 (ethernet0/0 interface), which is prebound to the Trust security zone.
2. Ensure that your workstation is configured with a static IP address in the 192.168.1.0/24 subnet.
3. Launch your browser, enter the IP address for the ethernet0/0 interface (the default IP address is 192.168.1.1), then press **Enter**.

The WebUI application displays the login prompt.

NOTE: When the device is accessed through the WebUI the first time, the Initial Configuration Wizard (ICW) appears. If you decide to use the ICW to configure your device, see “Initial Configuration Wizard” on page 53.

The WebUI application displays the login prompt.

4. If you have not yet changed the default login for the admin name and password, enter **netscreen** at both the admin name and password prompts. (Use lowercase letters only. The admin name and password fields are both case-sensitive.)
5. Once the WebUI homepage opens, the device is ready to be configured. See “Basic Device Configuration” on page 26 to complete the initial device configuration.

Using Telnet

To use a Telnet connection, the workstation must be in the same subnetwork as the security device. To access the device with a Telnet connection:

1. Connect your workstation to the port labeled 0/0 (ethernet0/0 interface), which is prebound to the Trust security zone.
2. Ensure that your workstation is configured with a static IP address in the 192.168.1.0/24 subnet.
3. Start a Telnet client application to the IP address for the ethernet0/0 interface (the default IP address is 192.168.1.1). For example, enter **telnet 192.168.1.1**.

The Telnet application displays the login prompt.

4. If you have not yet changed the default login for the login name and password, enter **netscreen** at both the login and password prompts. (Use lowercase letters only. The login and password fields are both case-sensitive)

5. (Optional) By default, the console times out and terminates automatically after 10 minutes of idle time. To prevent the console from timing out and terminating automatically, enter **set console timeout 0**.

Default Device Settings

Table 4 describes the default interface-to-zone bindings on the SSG 140 device.

Table 4: Default Interface-to-Zone Bindings

Port Label	Interface	Zone
10/100 Ethernet ports:		
0/0 (default IP address is 192.168.1.1/24)	ethernet0/0	Trust
0/1	ethernet0/1	DMZ
0/2	ethernet0/2	Untrust
0/3	ethernet0/3	Null
0/4	ethernet0/4	Null
0/5	ethernet0/5	Null
0/6	ethernet0/6	Null
0/7	ethernet0/7	Null
10/100/1000 Gigabit Ethernet ports:		
0/8	ethernet0/8	Null
0/9	ethernet0/9	Null

Note that the ethernet0/0 interface has the default IP address 192.168.1.1/24 and is configured for management services. If you connect the 0/0 port on the SSG 140 device to a workstation, you can configure the device from a workstation in the 192.168.1.1/24 subnetwork using a management service such as Telnet. You can change the default IP address on the ethernet0/0 interface to match the addresses on your LAN.

The SSG 140 comes preconfigured with three bridge group (bgroup) interfaces numbered bgroup0/0 through bgroup0/2. Bgroups let you group multiple Ethernet interfaces together. Each bgroup constitutes its own broadcast domain and provides high-speed Ethernet switching between interfaces within the group. You can assign a single IP address to each bgroup interface. You can bind a bgroup interface to any zone.

Basic Device Configuration

The following sections describe the basic configuration tasks required to place the SSG 140 device in operation.

- “Admin Name and Password” on page 26
- “Administrative Access” on page 27
- “Interface IP Address” on page 27
- “Management Services” on page 27
- “Hostname and Domain Name” on page 28
- “Domain Name System Server” on page 28
- “Date and Time” on page 28
- “Default Route” on page 29
- “Bridge Group Interfaces” on page 29

The examples in this section demonstrate how to establish initial network connectivity. For advanced configuration information, refer to the *Concepts & Examples ScreenOS Reference Guide*.

Admin Name and Password

The administrative user has complete privileges to configure a device. We recommend that you change the default admin name and password (both **netscreen**) immediately.

To change the admin name and password:

WebUI

Configuration > Admin > Administrators > Edit (for the NetScreen Administrator Name): Enter the following, then click **OK**:

Administrator Name:
Old Password: netscreen
New Password:
Confirm New Password:

CLI

```
set admin name name
set admin password pswd_str
save
```

Administrative Access

By default, anyone on your network who knows the login and password can manage your device.

To configure a device to be managed only from a specific host on your network:

WebUI

Configuration > Admin > Permitted IPs: Enter the following, then click **Add**:

IP Address/Netmask: *ip_addr/mask*

CLI

```
set admin manager-ip ip_addr/mask
save
```

Interface IP Address

The ethernet0/0 interface has the default IP address 192.168.1.1/24 and is preconfigured for management services. You can configure the device using a management service such as Telnet by connecting a workstation to the ethernet0/0 interface. The workstation must have an IP address in the 192.168.1.1/24 subnet.

To change the default interface IP address on the device:

WebUI

Network > Interfaces > Edit (for ethernet0/0): Enter the following, then click **OK**:

IP Address/Netmask: *ip_addr/mask*

CLI

```
set interface ethernet0/0 ip ip_addr/mask
save
```

Management Services

ScreenOS provides services for configuring and managing a device, such as SNMP, SSL, and SSH, which you can enable on a per-interface basis. You cannot configure WAN interfaces for management services.

To configure the management services for the ethernet0/0 interface:

WebUI

Network > Interfaces > Edit (for ethernet0/0): Under **Management Services**, select or clear the management services you want to use on the interface, then click **Apply**.

CLI

```
set interface eth0/0 manage web
unset interface eth0/0 manage snmp
save
```

Hostname and Domain Name

The domain name defines the network or subnetwork that the device belongs to, while the hostname refers to a specific device. The hostname and domain name together uniquely identify a device in the network.

To configure the hostname and domain name on the device:

WebUI

Network > DNS > Host: Enter the following, then click **Apply**:

Host Name: *hostname*
Domain Name: *domain-name*

CLI

```
set hostname hostname
set domain domain-name
save
```

Domain Name System Server

The Domain Name System (DNS) server on the network maintains a database for resolving hostnames and IP addresses. Devices access the configured DNS servers to resolve hostnames. In ScreenOS, you configure the IP addresses for the primary and secondary DNS servers and the time of the day at which the device performs a DNS refresh.

To configure the DNS server IP address:

WebUI

Network > DNS > Host: Enter the following, then click **Apply**:

Primary DNS Server: *ip_addr*
Secondary DNS Server: *ip_addr*
DNS Refresh: (select)
Every Day at: *time*

CLI

```
set dns host name ip_addr
set dns host name ip_addr
set dns host schedule time
save
```

Date and Time

The time settings on a device affect events such as the setup of virtual private network (VPN) tunnels. The easiest way to set the date and time on the device is to use the WebUI to synchronize the device clock with the clock on your workstation.

To configure the date and time on the device:

WebUI

1. Configuration > Date/Time: Click the Sync Clock with Client button.

A pop-up message prompts you to specify if you have enabled the daylight saving time option on your workstation clock.

2. Click **Yes** to synchronize the device clock and adjust it according to daylight saving time, or click **No** to synchronize the device clock without adjusting for daylight saving time.

You can also use the **set clock** command in a Telnet or console session to manually enter the date and time for the device.

Default Route

The default route is a static route used to direct packets addressed to networks that are not explicitly listed in the routing table. If a packet arrives at the device with an address for which the device does not have routing information, the device sends the packet to the destination specified by the default route. To configure the default route on the device:

WebUI

Network > Routing > Destination > New (trust-vr): Enter the following, then click **OK**:

Network Address/Netmask: 0.0.0.0/0.0.0.0
 Gateway: (select)
 Interface: ethernet0/2 (select)
 Gateway IP Address: *ip_addr*

CLI

```
set route 0.0.0.0/0 interface ethernet0/2 gateway ip_addr
save
```

Bridge Group Interfaces

The SSG 140 device is pre-configured with bridge group (bgroup) interfaces identified as bgroup0/0 through bgroup0/2.

Bgroups let you group multiple Ethernet interfaces together. Each bgroup constitutes its own broadcast domain and provides high-speed Ethernet switching between interfaces within the group. You can assign a single IP address to each bgroup interface. You can bind a bgroup interface to any zone.

You can unbind interfaces from a bridge group and assign them to a different security zone. Interfaces must be in the Null security zone before they can be bound to a bridge group. To bind a grouped interface to the Null security zone, use the **unset interface interface port interface** command.

To configure a bridge group:

WebUI

Network > Interfaces > List > Edit (bgroup0) > Bind Port: Select **ethernet0/3**, **ethernet0/4**, and **ethernet0/5**, then click **Apply**.

> Basic: Enter the following, then click **Apply**:

Zone Name: DMZ (select)
IP Address/Netmask: 10.0.0.1/24

CLI

```
set interface bgroup0/0 port ethernet0/3
set interface bgroup0/0 port ethernet0/4
set interface bgroup0/0 port ethernet0/5
set interface bgroup0/0 zone DMZ
set interface bgroup0/0 ip 10.0.0.1/24
save
```

If you want to bind an Ethernet interface to a bgroup, you must first make sure that the interface is in the Null security zone. Unsetting the interface that is in a bgroup places the interface in the Null security zone. Once assigned to the Null security zone, the Ethernet interface can be bound to a security zone and assigned a different IP address.

PIM Configuration

To configure the interfaces on physical interface modules (PIMs), refer to the *PIM and Mini-PIM Installation and Configuration Guide*.

Basic Firewall Protections

The devices are configured with a default policy that permits workstations in the Trust zone of your network to access any resource in the Untrust security zone, while outside computers are not allowed to access or start sessions with your workstations. You can configure policies that direct the device to permit outside computers to start specific kinds of sessions with your computers. For information about creating or modifying policies, refer to the *Concepts & Examples ScreenOS Reference Guide*.

SSG 140 devices provide various detection methods and defense mechanisms to combat probes and attacks aimed at compromising or harming a network or network resource:

- ScreenOS Screen options secure a zone by inspecting, and then allowing or denying, all connection attempts that require crossing an interface to that zone. For example, you can apply port-scan protection on the Untrust zone to stop a source from a remote network from trying to identify services to target for further attacks.

- The device applies firewall policies, which can contain content filtering and Intrusion Detection and Prevention (IDP) components, to the traffic that passes the Screen filters from one zone to another. By default, no traffic is permitted to pass through the device from one zone to another. To permit traffic to cross the device from one zone to another, you must create a policy that overrides the default behavior.

To set ScreenOS Screen options for a zone:

WebUI

Screening > Screen: Select the zone to which the options apply. Select the Screen options that you want, then click **Apply**:

CLI

```
set zone zone screen option
save
```

For more information about configuring the network security options available in ScreenOS, refer to the *Attack Detection and Defense Mechanisms* volume of the *Concepts & Examples ScreenOS Reference Guide*.

Verifying External Connectivity

To verify that workstations in your network can access resources on the Internet, start a browser from any workstation in the network and browse to www.juniper.net/.

Restarting the Device

You may need to restart the device in order to implement new features, such as when you change between route and transparent mode or when you add new license keys.

The following sections describe two methods of restarting the device:

- “Restarting the Device with the CLI Reset Command” on page 31
- “Restarting the Device with the WebUI” on page 32

Restarting the Device with the CLI Reset Command

To restart the device with the CLI reset command:

1. Establish a console session with the device as described in “Using a Console Connection” on page 28 or “Using Telnet” on page 30.

At a Windows workstation, the easiest way of opening a console connection is to choose **Start > Run** and enter **telnet ip_address**.

The device prompts you for your login and password.

2. If you have not yet changed the default username and password, enter **netscreen** at both the login and password prompts. (Use lowercase letters only. The login and password fields are both case-sensitive.)

3. At the console prompt, enter:

reset

The device prompts you to confirm the reset:

System reset, are you sure? y/[n]

4. Enter **Y**.

The device restarts.

Restarting the Device with the WebUI

To restart the device with the WebUI:

1. Launch your browser and enter the IP address for the management interface (the default IP address is **192.168.1.1**), then press **Enter**.

The WebUI application displays the login prompt.

2. If you have not yet changed the default username and password, enter **netscreen** at both the login and password prompts. (Use lowercase letters only. The login and password fields are both case-sensitive.)

3. In the WebUI, choose:

Configuration > Update > ScreenOS/Keys

4. Click **Reset**.

An alert box prompts you to confirm that you want to reset the device.

5. Click **OK**.

The device resets. Also, an alert box prompts you to leave your browser open for a few minutes and then log back into the device.

Resetting the Device to Factory Defaults

If you lose the admin password, or you need to clear the configuration of your device, you can reset the device to its factory default settings. Resetting the device destroys any existing configurations and restores access to the device.



CAUTION: Resetting the device deletes all existing configuration settings and disables all existing firewall and VPN services.

NOTE: By default, the device recovery feature is enabled. You can disable it by entering the CLI **unset admin device-reset** command. Also, if the security device is in FIPS mode, the recovery feature is automatically disabled.

You can restore the device to its default settings using one of these methods:

- Using the device serial number
- Using the CLI **unset all** command
- Using the Reset pinhole

The following sections describe how to use these methods to reset the device to its factory defaults.

Device Serial Number

To use the device serial number to reset the device to its factory defaults:

1. Start a Console session as described in “Using a Console Connection” on page 22.
2. At the Login prompt, enter the device serial number.
3. At the Password prompt, enter the serial number again. The following message appears:

```
!!! Lost Password Reset !!! You have initiated a command to reset the device to
factory defaults, clearing all current configuration and settings. Would you like to
continue? y/[n]
```

4. Press the **y** key. The following message appears:

```
!! Reconfirm Lost Password Reset !! If you continue, the entire configuration of the
device will be erased. In addition, a permanent counter will be incremented to
signify that this device has been reset. This is your last chance to cancel this
command. If you proceed, the device will return to factory default configuration,
which is: device IP: 192.168.1.1; username: netscreen, password: netscreen.
Would you like to continue? y/[n]
```

5. Press the **y** key to reset the device.

The system now resets and returns to the login prompt; the default login name and password are both reset to **netscreen**.

unset all

To use the CLI **unset all** command, you will need to know the login name and password. To reset the device to its factory defaults:

1. Start a Console session as described in “Using a Console Connection” on page 22, then log in.

2. At the command prompt, enter **unset all**. The following message is displayed:

```
Erase all system config, are you sure y/[n] ?
```

3. Press **y**
4. Enter **reset**. Press **n** for the first question and **y** for the second question:

```
Configuration modified, save? [y]/n
System reset, are you sure? y/[n]
```

The system now resets and returns to the login prompt; the default login name and password are both reset to **netscreen**.

Reset Pinhole Button

To use the Reset pinhole button (labeled Reset Config on some devices) on the device, you must either view the device status LEDs on the front panel or start a Console session.

NOTE: If you do not follow the complete sequence, the reset process cancels without any configuration change and the console message states that the erasure of the configuration is aborted. The Status LED returns to blinking green. The device generates SNMP and SYSLOG alerts to configured SNMP or SYSLOG trap hosts.

- Using the device status LEDs:

1. Locate the Reset (or Reset Config) pinhole on the device. Using a thin wire (such as a straightened paperclip), push the pinhole button for four to six seconds.

The Status LED blinks red.

2. As soon as the Status LED blinks green, release the pinhole button and wait two seconds.
3. The device now waits for the second reset, which confirms the operation. Push the pinhole button again for four to six seconds until the device resets.

The system now resets and returns to the login prompt; the default login name and password are both reset to **netscreen**.

- Using the Console:

1. Start a Console session as described in “Using a Console Connection” on page 22.
2. Locate the Reset pinhole on the device. Using a thin wire (such as a straightened paperclip), push the pinhole button for four to six seconds.

The message “Configuration Erasure Process has been initiated” appears in the console window. Continue to press the pinhole button until the message “Waiting for 2nd confirmation” appears.

3. Release the pinhole button, and wait two seconds.
4. Push the pinhole button again for four to six seconds.

The message “2nd push has been confirmed” appears.

5. Continue to press the pinhole button until the device resets.

The system now resets and returns to the login prompt; the default login name and password are both reset to **netscreen**.

Chapter 4

Servicing the Device

This chapter describes service and maintenance procedures for the SSG 140 device. It includes the following topics:

- “Tools and Parts Required” on page 37
- “Replacing a PIM” on page 38
- “Upgrading Memory” on page 40
- “Replacing the Fuse” on page 43

NOTE: For safety warnings and instructions, refer to the *Juniper Networks Security Products Safety Guide*. The instructions in the guide warn you about situations that could cause bodily injury. When working on any equipment, be aware of the hazards involved with electrical circuitry, and follow standard practices for preventing accidents.

Tools and Parts Required

To replace a component on an SSG 140 device, you need the following tools and parts:

- Electrostatic bag or antistatic mat
- Electrostatic discharge grounding wrist strap
- Flat-tip screwdriver, 1/8 inch
- Number-2 phillips screwdriver

Replacing a PIM

The SSG 140 device has four PIM slots in the back panel. PIMs are field installable and replaceable.



CAUTION: Power off the device before removing or installing PIMs. PIMs are not hot-swappable.

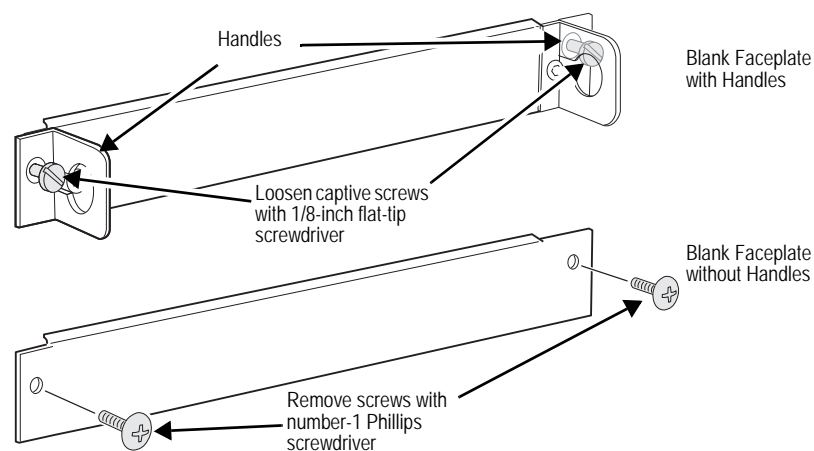
Removing a Blank Faceplate

To maintain proper airflow through the device, blank faceplates should remain over slots that do not contain PIMs. Do not remove blank faceplates unless you are installing a PIM in the empty slot.

To remove a blank faceplate:

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to the ESD point on the device.
2. If the device is powered on, switch off the power switch on the back of the device. Verify that the POWER LED is off.
3. Loosen the screws on each side of the faceplate as shown in Figure 10:
 - On faceplates with handles, use a 1/8-inch flat-tip screwdriver to loosen but do not remove the captive screws.
 - On faceplates without handles, use a number-1 phillips screwdriver to remove the non-captive screws.

Figure 10: Identifying Blank Faceplate Types



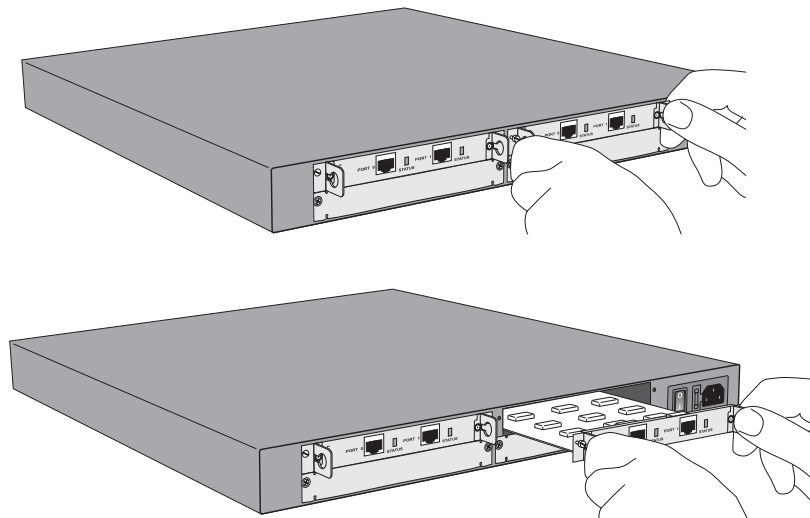
4. Remove the faceplate.

Removing a PIM

To remove a PIM:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface on which you intend to place the PIM.
2. Attach an ESD grounding strap to your bare wrist, and connect the strap to an ESD point on the device.
3. If the device is powered on, switch off the power switch on the back of the device. Verify that the POWER LED is off.
4. Label the cables connected to the PIM so that you can later reconnect each cable to the correct PIM.
5. Disconnect the cables from the PIM.
6. If necessary, arrange the cables to prevent them from dislodging or developing stress points.
7. Loosen the captive screws on each side of the PIM using a 1/8-inch flat-tip screwdriver.
8. Grasp the handles on each side of the PIM faceplate, and slide the PIM out of the device (see Figure 11). On some PIMs the handles are metal ears attached to the PIM faceplate. Other PIMs have long screws that serve as the handles.

Figure 11: Removing/Installing a PIM



9. Place the PIM in the electrostatic bag or on the antistatic mat.
10. If you are not reinstalling a PIM into the empty slot, install a blank PIM faceplate over the slot to maintain proper airflow.

Installing a PIM

To install a PIM:

1. Attach an ESD grounding strap to your bare wrist, and connect the strap to the ESD point on the device.
2. If the device is powered on, switch off the power switch on the back of the device. Verify that the POWER LED is off.
3. Grasp the handles on each side of the PIM faceplate. On some PIMs the handles are metal ears attached to the PIM faceplate. Other PIMs have long screws that serve as the handles.
4. Align the edges of the PIM circuit board with the guide rails at each side of the PIM slot.
5. Slide the PIM in until it seats firmly in the device.



CAUTION: Slide the PIM straight into the slot to avoid damaging the components on the PIM.

6. Tighten the screws on each side of the PIM faceplate:
 - On PIMs with metal ear handles attached to the faceplate, tighten the captive screws using a 1/8-inch flat-tip screwdriver.
 - On PIMs with long screws for handles, tighten the captive screws using a number-2 phillips screwdriver.
7. Insert the appropriate cables into the cable connectors on the PIM.
8. If necessary, arrange the cables to prevent them from dislodging or developing stress points:
 - Secure the cable so that it is not supporting its own weight as it hangs to the floor.
 - Place excess cable out of the way in a neatly coiled loop.
 - Use fasteners to maintain the shape of cable loops.
9. Power on the device. Verify that the POWER LED lights steadily after you press the power button.
10. Verify that the PIM status LED lights steadily green to confirm that the PIM is online.

Upgrading Memory

You can upgrade an SSG 140 device that has 256 MB of memory to 512 MB by replacing the 256 MB memory module with a 512 MB memory module. Ask your Juniper reseller for kit SSG-100-MEM-512.

To determine the amount of memory, use the **get sys** command. The command response shows the amount of memory installed.

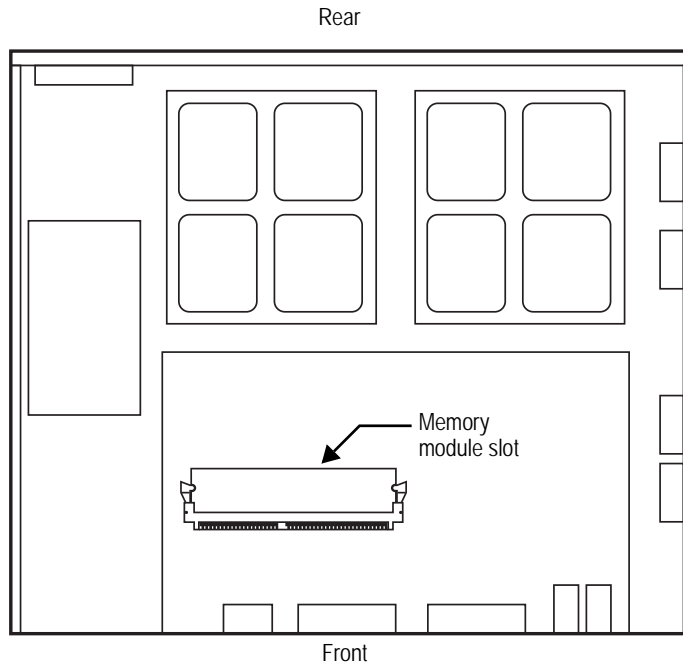
NOTE: The SSG 140 device must have 512 MB of memory installed to run the following ScreenOS Unified Threat Management (UTM) features:

- Antivirus
 - Antispam
 - Web filtering
 - Intrusion Prevention System (IPS)
-

To upgrade the memory on the SSG 140 device:

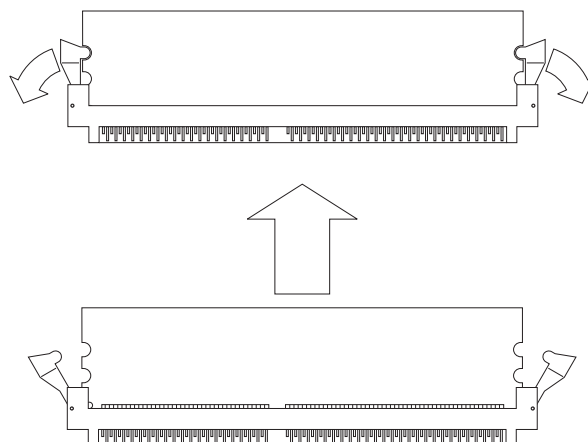
1. Attach an ESD grounding strap to your bare wrist, and connect the strap to the ESD point on the chassis or to an outside ESD point if the device is disconnected from earth ground.
2. Power off the device. Verify that the POWER LED turns off.
3. Remove the device from its rack mount.
4. Use a number-2 phillips screwdriver to remove the screws securing the rack mount brackets to the sides of the unit (four screws per side).
5. Use the phillips screwdriver to remove the six countersunk screws located along the bottom edge of the side of the unit (three screws per side).
6. Use the phillips screwdriver to remove the countersunk screws located at each end of the front panel of the unit (two screws).
7. Grip the cover and slide it forward about 1/2-inch (13mm).
8. Lift the cover off and remove it.
9. Locate the memory module slot as shown in Figure 12.

Figure 12: Memory Module Slot



10. Release the 256 MB memory module by pressing your thumbs downward on the locking tabs on each side of the module so that the tabs swivel away from it.
11. Grip the long edge of the memory module and slide it out. Set it aside.

Figure 13: Releasing and Removing the Memory Module



12. Insert the 512 MB memory module into the slot from which you removed the 256 MB memory module. Exerting even pressure with both thumbs upon the upper edge of the module, press the module downward until the locking tabs click into position.

13. To replace the top panel on the chassis, set the rear edge of the top panel into the groove that runs along the top rear edge of the chassis. Then lower the top panel onto the chassis.
14. Slide the top panel back 1/2-inch (13mm).
15. Use the number-2 phillips screwdriver to replace and tighten the screws you removed earlier, securing the top panel to the chassis.
16. Use the screwdriver to replace and tighten the screws securing the rack mount brackets to the sides of the chassis.
17. Replace the SSG 140 in the equipment rack.

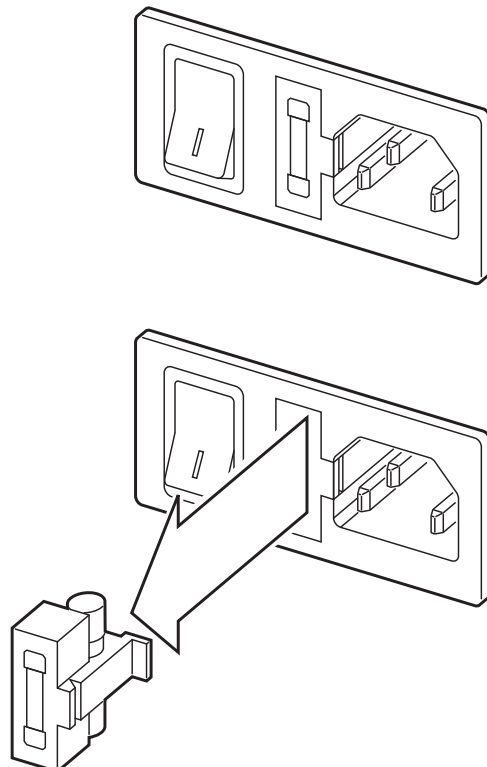
Replacing the Fuse

The SSG 140 device uses a 6.3 amp fast acting fuse rated for 250 volts.

To replace a failed fuse on the SSG 140 device:

1. Take the device off-line, turn the power switch OFF, and disconnect the power cable.
2. Using a flat-tip screwdriver, separate the lid of the external fuse cover from the surface of the power outlet.

Figure 14: Removing the Fuse



3. Manually remove the fuse assembly from the device.
4. To replace the fuse assembly, enter the new fuse into the opening and slide it in until the fuse clicks into place.
5. Replace the power cable and turn the device power switch ON. Reconnect the network cables.

Appendix A

Specifications

This appendix provides general specifications for the SSG 140 device. It contains the following sections:

- “Physical” on page 45
- “Electrical Specifications” on page 46
- “Environmental Tolerance” on page 46
- “Certifications” on page 47
- “Connectors” on page 48

Physical

Table 5 provides the physical specifications for the SSG 140 device.

Table 5: SSG 140 Physical Specifications

Description	Value
Chassis dimensions	1.75 inches (4.4 cm) high
	17.5 inches (44.4 cm) wide—18.9 in. (48 cm) wide with mounting brackets attached
	15 inches (38.1 cm) deep—plus 0.5 in. (1.27 cm) of hardware that protrudes from the chassis front
Device weight	Minimum configuration (no PIMs): 10.2 lbs (4.6 kg)
	Maximum configuration (four PIMs): 11.7 lbs (5.3 kg)

Electrical Specifications

Table 6 provides the electrical specifications for the SSG 140 device.

Table 6: SSG 140 Electrical Specifications

Item	Specification
AC input voltage	Operating range: 90 to 264 VAC
AC input line frequency	50 or 60 Hz
AC device current rating	1.8A

Environmental Tolerance

Table 7 provides the environmental tolerance for the SSG 140 device.

Table 7: SSG 140 Environmental Tolerance

Description	Value
Altitude	No performance degradation to 6560 ft (2000 m)
Relative humidity	Normal operation ensured in relative humidity range of 5 % to 90 %, noncondensing
Temperature	Normal operation ensured in temperature range of 32°F (0°C) to 104°F (40°C) Non-operating storage temperature in shipping carton: -40°F (-40°C) to 158°F (70°C)
Maximum thermal output	580 BTU/hour (170 W)

Certifications

Table 8 provides the device certifications for the SSG 140 device.

Table 8: SSG 140 Device Certifications

Certification Type	Certification Name
Safety	CAN/CSA-C22.2 No. 60950-1-03/UL 60950-1 Safety of Information Technology Equipment
	EN 60950-1 Safety of Information Technology Equipment
	EN 60825-1 Safety of Laser Products - Part 1
EMC Emissions	FCC Part 15 Class B (USA)
	EN 55022 Class B (Europe, Australia, New Zealand)
	VCCI Class B (Japan)
	BSMI Class B (Taiwan)
EMC Immunity	EN 55024
	EN-61000-3-2 Power Line Harmonics
	EN-61000-3-3 Voltage Fluctuations and Flicker
	EN-61000-4-2 ESD
	EN-61000-4-3 Radiated Immunity
	EN-61000-4-4 EFT
	EN-61000-4-5 Surge
	EN-61000-4-6 Low Frequency Common Immunity
ETSI	EN-61000-4-11 Voltage Dips and Sags
T1 Interface	European Telecommunications Standards Institute (ETSI) EN-300386-2: Telecommunication Network Equipment. Electromagnetic Compatibility Requirements (equipment category Other than telecommunication centers)
	FCC Part 68 - TIA 968
	Industry Canada CS-03
	UL 60950-1 -Evaluated to applicable requirements for TNV-1 circuit

Connectors

Figure 15 shows the pin numbering of the RJ-45 connectors for the Console and AUX ports.

Figure 15: RJ-45 Connector Pin Numbering

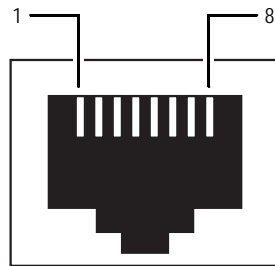


Table 9 lists the pinouts of the RJ-45 connectors for the Console and AUX ports.

Table 9: Console and AUX RJ-45 Connector Pinouts

Pin	Name	I/O	Description
1	RTS Out	O	Request To Send
2	DTR Out	O	Data Terminal Ready
3	TxD	O	Transmit Data
4	GND	-	Chassis Ground
5	GND	-	Chassis Ground
6	RxD	I	Receive Data
7	DSR	I	Data Set Ready
8	CTS	I	Clear To Send

Figure 16 shows the pin numbering of the connector on the DB-9 adapter supplied with the device.

Figure 16: DB-9 Connector Pin Numbering

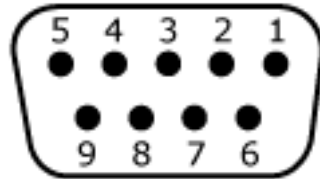


Table 10 lists the pinouts for the DB-9 adapter.

Table 10: DB-9 Adapter Pinouts

DB-9 Pin	RJ-45 Pin	Name	I/O	Description
1	N/C	DCD	< -	Carrier Detect
2	3	RxD	< -	Receive Data
3	6	TxD	- >	Transmit Data
4	7	DTR	- >	Data Terminal Ready
5	4	Ground	-	Signal Ground
6	2	DSR	< -	Data Set Ready
7	8	RTS	- >	Request To Send
8	1	CTS	< -	Clear To Send
9	N/C	RING	< -	Ring Indicator

Table 11 lists the RJ-45 connector pinouts for the Gigabit Ethernet ports.

Table 11: Gigabit Ethernet RJ-45 Connector Pinout

Pin	Signal
1	MDI0 +
2	MDI0-
3	MDI1 +
4	MDI2 +
5	MDI2-
6	MDI1-
7	MDI3 +
8	MDI3-

The E1 and T1 PIMs use RJ-48 cables, which are not supplied with the PIM. Table 12 describe the RJ-48 connector pinouts.



CAUTION: To maintain agency approvals, use only properly constructed, shielded cables.

Table 12: RJ-48 Connector to RJ-48 Connector (Straight) Pinout

RJ-48 Pin (on T1/E1 PIM) (Data Numbering Form)	Signal
1	RX, Ring, -
2	RX, Tip, +
4	TX, Ring, -
5	TX, Tip, +

Appendix B

Initial Configuration Wizard

This appendix provides detailed information about the Initial Configuration Wizard (ICW) for an SSG 140 device.

After you have physically connected your device to the network, you can use the ICW to configure the interfaces that are installed on your device.

This section describes the following ICW windows:

1. Rapid Deployment Window on page 52
2. Administrator Login Window on page 52
3. Physical Ethernet Interface Window on page 53
4. Untrust Zone Window on page 54
5. DMZ Interface IP Address Window on page 55
6. Trust Interface IP Address Window on page 55
7. Physical Ethernet DHCP Interface Window on page 56
8. Confirmation Window on page 57

1. Rapid Deployment Window

Figure 17: Rapid Deployment Window

If your network uses Network and Security Manager (NSM), you can use a Rapid Deployment configlet to automatically configure the device. Obtain a configlet from your Security Manager administrator, select the **Yes** option, select the **Load Configlet from:** option, browse to the file location, then click **Next**. The configlet sets up the device for you.

If you want to bypass the configuration wizard and go directly to the WebUI, select the last option, then click **Next**.

If you are not using a configlet to configure the device and want to use the configuration wizard, select the first option, then click **Next**. The ICW welcome screen appears. Click **Next**. The Administrator Login Window appears.

2. Administrator Login Window

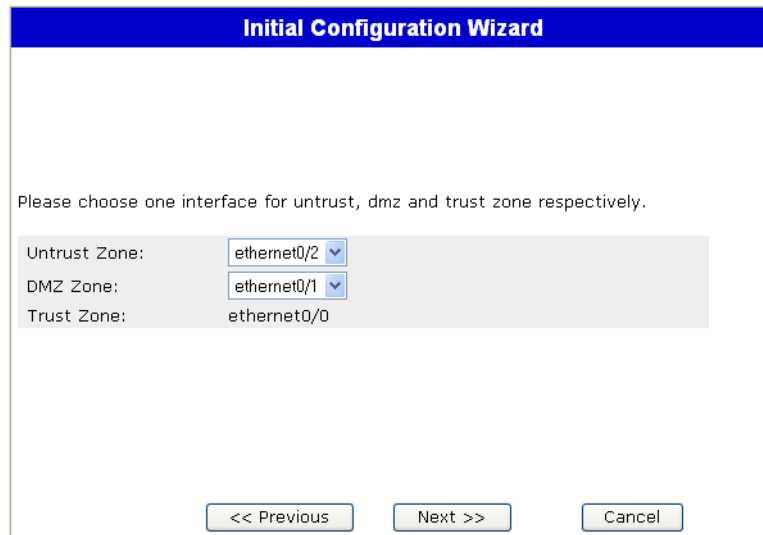
Enter a new administrator login name and password, then click **Next**.

Figure 18: Admin Login Window

3. Physical Ethernet Interface Window

On the interface-to-zone bindings screen, you set the interface to which you want to bind the Untrust security zone. Ethernet0/0 is prebound to the Trust security zone. Ethernet0/1 is bound to the DMZ security zone but is optional. Ethernet0/2 is bound to the Untrust zone.

Figure 19: Physical Ethernet Interface Window



The screenshot shows a window titled "Initial Configuration Wizard". Inside the window, there is a text prompt: "Please choose one interface for untrust, dmz and trust zone respectively." Below this prompt, there are three rows of configuration options:

Untrust Zone:	ethernet0/2
DMZ Zone:	ethernet0/1
Trust Zone:	ethernet0/0

At the bottom of the window, there are three buttons: "<< Previous", "Next >>", and "Cancel".

After binding an interface to a zone, you can configure the interface. Depending on which interfaces you have installed on your device, mini PIM-specific configuration windows are displayed. To continue configuring your device with the ICW, click **Next**.

4. Untrust Zone Window

The Untrust zone interface can have a static IP address or a dynamic IP address assigned via DHCP. Insert the desired information, then click **Next**.

Figure 20: Untrust Zone Window

Table 13: Field Descriptions for Ethernet0/0 Interface

Field	Description
Dynamic IP via DHCP	Enables the device to receive an IP address for the Untrust zone interface from an ISP.
Dynamic IP via PPPoE	Enables the device to act as a PPPoE client, receiving an IP address for the Untrust zone interface from an ISP. Enter the username and password assigned by the ISP.
Static IP	Assigns a unique and fixed IP address to the Untrust zone interface. Enter the Untrust zone interface IP, Netmask, and gateway.

5. DMZ Interface IP Address Window

Use this screen to configure an IP address and a netmask for the DMZ interface.

Figure 21: DMZ Interface IP Address Window

The screenshot shows a window titled "Initial Configuration Wizard" with a blue header. Below the header, the text reads "Enter the IP address and netmask for the interface ethernet0/1 (DMZ zone)". There are two radio button options: "Dynamic IP via DHCP" (unselected) and "Static IP" (selected). Under the "Static IP" option, there are two input fields: "Interface IP:" with the value "10.100.37.235" and "Netmask:" with the value "255.255.255.0". At the bottom of the window, there are three buttons: "<< Previous", "Next >>", and "Cancel".

6. Trust Interface IP Address Window

Use this screen to configure an IP address and a netmask for the Trust interface.

Figure 22: Trust Interface IP Address Window

The screenshot shows a window titled "Initial Configuration Wizard" with a blue header. Below the header, the text reads "Enter the IP address and netmask for the interface ethernet0/0 (Trust zone)". There are two radio button options: "Dynamic IP via DHCP" (unselected) and "Static IP" (selected). Under the "Static IP" option, there are two input fields: "Interface IP:" with the value "10.100.23.2" and "Netmask:" with the value "255.255.255.0". At the bottom of the window, there are three buttons: "<< Previous", "Next >>", and "Cancel".

7. Physical Ethernet DHCP Interface Window

Select **Yes** to enable your device to assign IP addresses to your wired network via DHCP. Enter the IP address range that you want your device to assign to clients using your network, then click **Next**.

Figure 23: Ethernet DHCP Interface Window

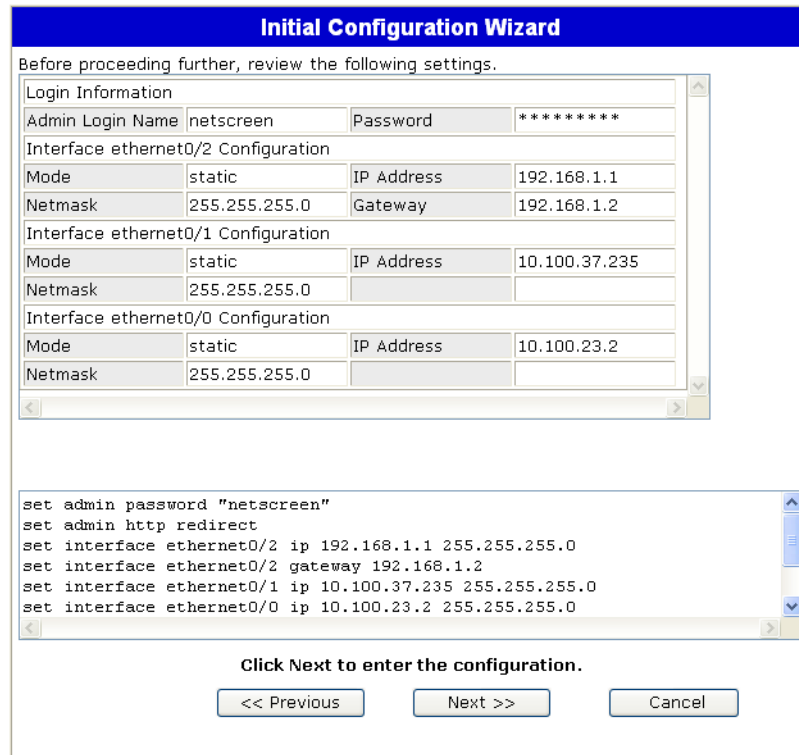
The screenshot shows a window titled "Initial Configuration Wizard" with a blue header. The main text asks: "Do you want the Juniper device to dynamically assign IP addresses to your local **wired** hosts using DHCP? If so, select Yes and enter an IP address range from which to assign the addresses." Below this is a form with two radio buttons: "Yes" and "No". The "No" option is selected. Under the "Yes" option, there are four input fields: "IP Address Range Start" (192.168.1.33), "End" (192.168.1.126), "DNS Server 1 (optional)", and "DNS Server 2 (optional)". At the bottom are three buttons: "<< Previous", "Next >>", and "Cancel".

Initial Configuration Wizard	
Do you want the Juniper device to dynamically assign IP addresses to your local wired hosts using DHCP? If so, select Yes and enter an IP address range from which to assign the addresses.	
<input type="radio"/> Yes	
IP Address Range Start	<input type="text" value="192.168.1.33"/>
End	<input type="text" value="192.168.1.126"/>
DNS Server 1	(optional) <input type="text"/>
DNS Server 2	(optional) <input type="text"/>
<input checked="" type="radio"/> No	
<input >="" ><="" <input="" td="" type="button" value=" Cancel "/>	

8. Confirmation Window

Confirm your device configuration and change as needed. Click **Next** to save, restart the device, and run the configuration.

Figure 24: Confirmation Window



Initial Configuration Wizard

Before proceeding further, review the following settings.

Login Information			
Admin Login Name	netscreen	Password	*****

Interface ethernet0/2 Configuration			
Mode	static	IP Address	192.168.1.1
Netmask	255.255.255.0	Gateway	192.168.1.2

Interface ethernet0/1 Configuration			
Mode	static	IP Address	10.100.37.235
Netmask	255.255.255.0		

Interface ethernet0/0 Configuration			
Mode	static	IP Address	10.100.23.2
Netmask	255.255.255.0		

```

set admin password "netscreen"
set admin http redirect
set interface ethernet0/2 ip 192.168.1.1 255.255.255.0
set interface ethernet0/2 gateway 192.168.1.2
set interface ethernet0/1 ip 10.100.37.235 255.255.255.0
set interface ethernet0/0 ip 10.100.23.2 255.255.255.0

```

Click Next to enter the configuration.

<< Previous Next >> Cancel

After the device restarts with the saved system configuration, the WebUI login prompt appears. For information about accessing the device using the WebUI, see “Using the WebUI” on page 24.

Index

A

access, configuring administrative	27
addresses, default IP	25
admin name and password, changing.....	26
administrative access, configuring	27
ALARM LED	11

B

back-panel components.....	13
basic configuration	26
before you begin.....	16
bgroups, configuring	29
bindings, default port and zone	25
bridge groups, configuring.....	29

C

certifications.....	47
components, device	13
configuration	
admin name and password	26
administrative access	27
basic steps.....	26
bridge group (bgroup).....	29
date and time	28
default routes.....	29
DNS server	28
hostname and domain name	28
management services.....	27
USB	12
connecting power	18

D

date and time, configuring	28
default routes, configuring.....	29
device	
certifications	47
configuration.....	26
dimensions.....	45
weight	45
device LEDs.....	11
dimensions of device	45
DNS servers, configuring	28

E

electrical specifications.....	46
--------------------------------	----

EMC certifications.....	47
emissions certifications.....	47
environmental specifications	46
equipment racks, installing.....	16

F

faceplates, removing	38
factory defaults, resetting to	32

H

HA LED	11
hostnames and domain names, configuring.....	28

I

immunity certifications.....	47
installation	
before you begin	16
connecting power.....	18
equipment racks.....	16
PIMs	40
IP addresses, default.....	25

L

LEDs	
activity link on Ethernet ports	12
dashboard	11
LAN ports	12

M

management	
Telnet.....	24
WebUI.....	24
management services, configuring.....	27
managing	
through WebUI	31, 32
memory, upgrading	41

P

PIM LEDs	11
PIMs	
installing	40
removing	39
port bindings, default	25
POWER LED	11
power switch	14

power, connecting 18

R

racks, installing 16
 removing
 faceplates 38
 PIMs 39
 Reset/Reset Config button 34
 resetting to factory defaults 32
 restarting the device 31
 routes, configuring default 29

S

safety certifications 47
 services, configuring management 27
 specifications
 electrical 46
 environmental 46
 physical 45
 STATUS LED 11

T

Telnet, managing with 24

U

USB, configuration 12

W

WebUI, managing with 24
 WebUI, using 31, 32
 weight, of device 45

Z

zones, default bindings 25