SSG20 Hardware and Installation Guide

Important:

We are providing the following guide as a courtesy, but no longer support the documented product. The SSG20 firewall reached end of service in January 2020.

For information about a currently supported firewall that might better suit your needs, we recommend the SRX300 Services Gateway.

Security Products

SSG 20 Hardware Installation and Configuration Guide

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

Part Number: 530-015646-01, Revision 07

Copyright 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

The Juniper Networks Secure Services Gateway (SSG) 20 device is an integrated router and firewall platform that provides Internet Protocol Security (IPSec) virtual private network (VPN) and firewall services for a branch office or a retail outlet.

Juniper Networks offers two models of the SSG 20 device:

- SSG 20, which supports auxiliary (AUX) connectivity
- SSG 20-WLAN, which supports integrated 802.11a/b/g wireless standards

---

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 http://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 sections:

- Chapter 1, “Hardware Overview,” describes the chassis and components of the SSG 20 device.
- Chapter 2, “Installing and Connecting the Device,” describes how to mount the SSG 20 device and how to connect cables and power to the device.
- Chapter 3, “Configuring the Device,” describes how to configure and manage the SSG 20 device and how to perform some basic configuration tasks.
- Chapter 4, “Servicing the Device,” describes service and maintenance procedures for the SSG 20 device.
- Appendix A, “Specifications,” provides general system specifications for the SSG 20 device.
- Appendix B, “Initial Configuration Wizard,” provides detailed information about using the Initial configuration Wizard (ICW) for the SSG 20 device.
- Appendix C, “Country Code and Channel Information,” provides information regarding wireless network deployment.

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

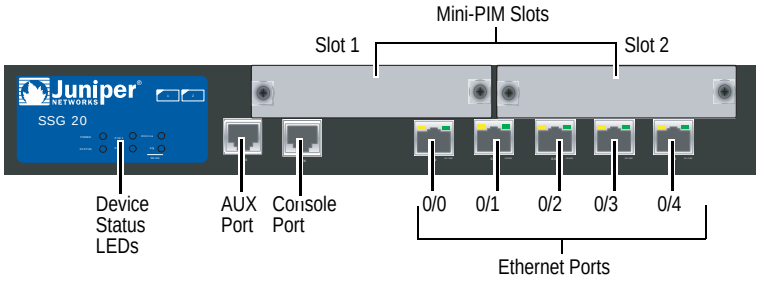
Hardware Overview

This chapter provides detailed descriptions of the SSG 20 chassis and its components. It contains the following sections:

Front Panel

Figure 1 shows the front panel of the SSG 20 device.

Figure 1: SSG 20 Front Panel



The following sections describe the elements on the front panel of the SSG 20 device:

Port Descriptions

Table 1 describes the function, connector type, and speed/protocol (if applicable) of each element on the front panel of the SSG 20 device.

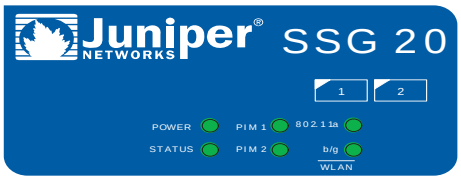
Table 1: SSG 20 Ports

Item	Description	Connector	Speed/Protocol
Ethernet 0/0 to 0/4 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 **ethernet0/4**. For the default zone bindings for each Ethernet port, see "Default Device Settings" on page 27.	RJ-45	10/100 Mbps Ethernet Autosensing duplex and auto MDI/MDIX
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 51 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 51 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 20-WLAN device. The WLAN LEDs are only present on the SSG 20-WLAN device.

Figure 2: Device Status LEDs (SSG 20-WLAN Shown, SSG 20 Similar)



When the device powers up, the POWER LED changes from off to blinking green, and the STATUS LED changes in the following sequence: red, green, blinking green. Startup takes approximately two minutes 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	Indicates that the device is receiving power.
		Off	Indicates that the device is not receiving power.
	Red	On steadily	Indicates that the device is not operating normally.
		Off	Indicates that the device is operating normally.
STATUS	Green	On steadily	Indicates that the device is starting or performing diagnostics.
		Blinking	Indicates that the device is operating normally.
	Red	Blinking	Indicates that there is an error detected.
PIM 1	Green	On steadily	Indicates that the Mini-PIM is functioning.
		Blinking	Indicates that the Mini-PIM is passing traffic.
		Off	Indicates that the Mini-PIM is not operational.
PIM 2	Green	On steadily	Indicates that the Mini-PIM is functioning.
		Blinking	Indicates that the Mini-PIM is passing traffic.
		Off	Indicates that the Mini-PIM is not operational.

Table 2: Device Status LED Descriptions (Continued)

Name	Color	Status	Description
WLAN (On WLAN device only)			
802.11a	Green	On steadily	Indicates that a wireless connection is established but there is no link activity.
		Blinking slowly	Indicates that a wireless connection is established. The baud rate is proportional to the link activity.
		Off	Indicates that there is no wireless connection established.
b/g	Green	On steadily	Indicates that a wireless connection is established but there is no link activity.
		Blinking slowly	Indicates that a wireless connection is established. The baud rate is proportional to the link activity.
		Off	Indicates that there is no wireless connection established.

Ethernet Port LEDs

The Ethernet port 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

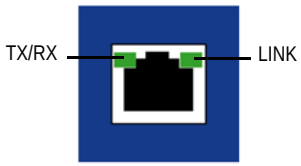


Table 3 describes the Ethernet port LEDs.

Table 3: Ethernet Port LEDs

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

Mini-Physical Interface Module Slots

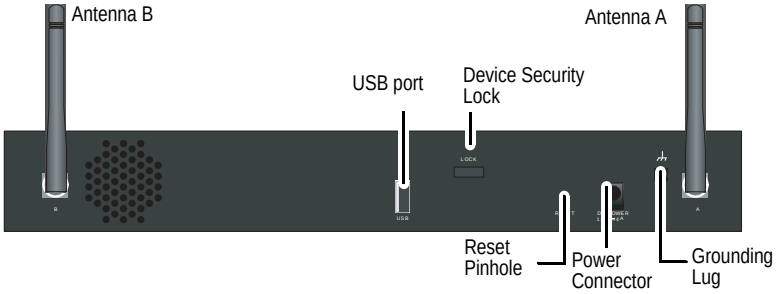
Mini-physical interface modules (mini-PIMs) let you add Ethernet and WAN interfaces to your SSG 20 device. To install and remove PIMs, see "Replacing Mini-Physical Interface Modules" on page 44. For more information about installing and configuring Mini-PIMs, refer to the *PIM and Mini-PIM Installation and Configuration Guide.*

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

Back Panel

Figure 4 shows the back panel of the SSG 20 device.

Figure 4: Back Panel of the SSG 20 Device (SSG 20-WLAN Shown)



The following sections describes the elements on the back panel of the SSG 20 device:

- Power Connector
- Radio Transceivers on page 14
- Grounding Lug on page 14
- Antennae Types on page 14
- USB Port on page 14

Power Connector

The power connector lets you connect the device to the AC power adapter supplied with the device. (We recommend using a surge protector.)

NOTE: The POWER LED on the front panel of the device glows green when power is connected properly.

Radio Transceivers

The SSG 20 wireless transceivers enable a direct connection to workstations in the vicinity of a wireless radio connection. Table 4 shows information for the transceivers.

Table 4: Radio Transceiver Information

Transceivers	Radio Band	Standard	Speed
WLAN 0	2.4 GHz	802.11b	11 Mbps
	2.4 GHz	802.11g	54 Mbps
	2.4 GHz and 5GHz	802.11 superG	108 Mbps
WLAN 1	5GHz	802.11a	54 Mbps

For information on configuring the wireless radio band, see “Basic Wireless Configuration” on page 33.

Grounding Lug

Use the one-hole grounding lug on the back of the device to connect the device to earth ground (see Figure 4).

To ground the device before connecting power, connect a grounding cable to earth ground and then attach the cable to the lug on the rear of the chassis.

Antennae Types

The SSG 20-WLAN device supports three types of custom-built radio antennae:

- **Diversity antennae** — The diversity antennae provide 2dBi directional coverage and a fairly uniform level of signal strength within the area of coverage and are suitable for most installations. This type of antennae is shipped with the device.
- **External omnidirectional antenna** — The external antenna provides 2dBi omnidirectional coverage. Unlike diversity antennae, which function as a pair, an external antenna operates to eliminate an echo effect that can sometimes occur from slightly delayed characteristics in signal reception when two are in use.
- **External directional antenna** — The external directional antenna provides 2dBi unidirectional coverage and is appropriate for locations like hallways and outer walls (with the antenna facing inward).

USB Port

The USB port on the back panel of an SSG 20 device accepts a universal serial bus (USB) storage device.

The USB port lets 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 port supports 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 the USB storage device and an SSG 20:

1. Connect the USB storage device to the 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 on the USB storage device and internal flash storage, use the **get file** command.

Chapter 2

Installing and Connecting the Device

This chapter describes how to mount the SSG 20 device and connect cables and power to the device. This chapter contains the following sections:

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

WARNING: To prevent abuse and intrusion by unauthorized personnel, install the SSG 20 device in a secure environment.

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

- Before installation, always check that the power supply is disconnected from any power source.
- Ensure that the room in which you operate the device has adequate air circulation and has a room temperature range of 32°F (0°C) to 104°F (40°C).
- Do not place the device in an equipment-rack frame that blocks an intake or exhaust port. Ensure that enclosed racks have fans and louvered sides.
- Correct these hazardous conditions before any installation: moist or wet floors, leaks, ungrounded or frayed power cables, or missing safety grounds.

Installing Equipment

The following sections describe how to rack-mount, wall-mount, or desk-mount the SSG 20 device:

- “Rack Mount” on page 19
- “Wall Mount” on page 19
- “Desk Mount” on page 20

The mounting kits may be purchased separately.

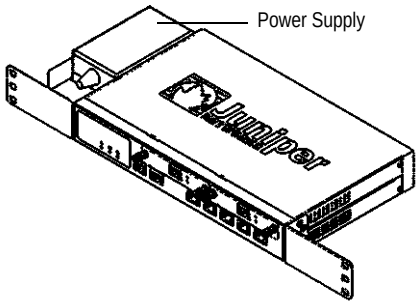
To rack-mount the SSG 20 device, you must have a Number-2 phillips screwdriver (not provided) and screws that are compatible with the equipment rack (included in the kit).

NOTE: When mounting the device, make sure that it is within reach of the power outlet.

Rack Mount

Figure 5 shows the SSG 20 device with rack mount brackets attached, ready to install in an equipment rack.

Figure 5: SSG 20 Rack-mount



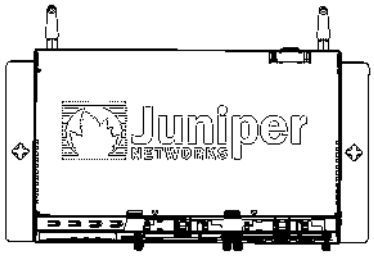
To rack-mount the SSG 20 device in a standard 19-inch equipment rack:

1. Align the power supply rack-mount ear to the left-front edge of the device.
2. Place the screws in the holes and use a phillips screwdriver to secure them.
3. Align the other rack-mount ear to the right-front edge of the device.
4. Place the screws in the holes and use a phillips screwdriver to secure them.
5. Mount the device on the rack with the provided screws.
6. Plug the power supply into the power outlet.

Wall Mount

Figure 6 shows the SSG 20 device with wall mount brackets attached, ready to attach to a wall.

Figure 6: SSG 20 Wall-mount



To wall-mount the SSG 20 device:

1. Align the wall-mount ears to the device.
2. Place the screws in the holes and use a phillips screwdriver to secure them.
3. Ensure that the wall to be used is smooth, flat, dry, and sturdy.

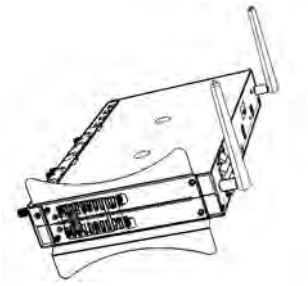
4. Mount the device on the wall using the provided screws.

5. Plug the power supply into the power outlet.

Desk Mount

Figure 7 shows the SSG 20 device with desk mount bracket attached, ready to be placed on a desktop.

Figure 7: SSG 20 Desk-mount



To desk-mount the SSG 20 device:

1. Attach the desktop stand to the side of the device. We recommend using the side closest to the power adapter.

2. Place the mounted device on the desktop.

3. Plug in the power adapter and connect the power supply to the power outlet.

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

To connect the power to a device:

1. Plug the DC-connector end of the power cable into the DC-power receptacle on the back of the device.
2. Plug the AC-adapter end of the power cable into an AC-power source.

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

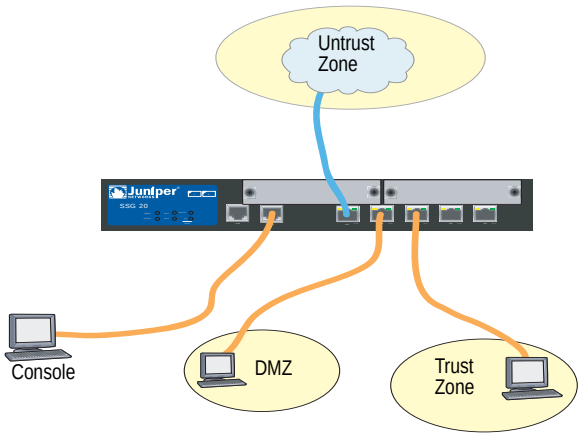
Connecting the Device to a Network

This section provides basic information on how to physically connect the SSG 20 device to a network.

To connect the necessary cables as shown in Figure 8, perform the following steps:

1. Connect an RJ-45 cable from the port labeled **0/0** (ethernet0/0 interface) to the external switch or router. The ethernet0/0 interface is prebound to the Untrust 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** (bgroup0 interface) to a switch or router in the Trust security zone.
4. Connect an RJ-45 cable from the Console port using the instructions provided in “Using a Console Connection” on page 24 for management access.

Figure 8: Basic Networking Example



5. If you want to connect to your device through wireless, you must first connect the provided antennae to the device. If you have the standard 2dB diversity antennae, use screws to attach them onto the RPSMA posts marked A and B at the back of the device. Bend each antenna at its elbows, making sure not to put pressure on the bulkhead connectors (see Figure 9).

Figure 9: SSG 20-WLAN Antennae Location

If you are using the optional external antenna, follow the connection instructions that came with that antenna.

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 SSG 20 devices. 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 need to perform further configuration for your specific network requirements.

This chapter contains the following sections:

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 *Fundamentals* volume of the *Concepts & Examples ScreenOS Reference Guide* for the ScreenOS version running on the device.

Accessing the Device

You can configure and manage the SSG 20 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 24.

- **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 subnetwork 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.

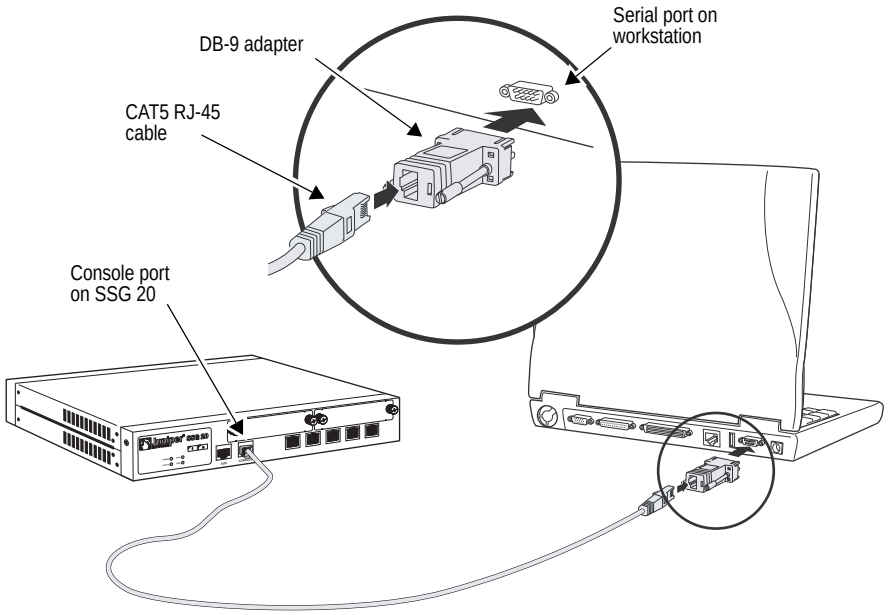
To establish a console connection with the device:

1. Plug the female end of an RJ-45-to-DB-9 adatper into the serial port of your workstation, making sure it is properly secured. (RJ-45-to-DB-9 adapters can be purchased from Juniper Networks. See "Connectors" on page 51 for pin numbering information.)

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 20 device. Figure 10 shows the arrangement of the cable and adapter.

Figure 10: 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 on how to configure the device with the 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**.

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 0/2 — 0/4 port (bgroup0 interface in the Trust zone) on the device.

2. Ensure that your workstation is configured for Dynamic Host Configuration Protocol (DHCP) or is statically configured with an IP address in the 192.168.1.0/24 subnet.

3. Launch your browser, enter the IP address for the bgroup0 interface (the default IP address is 192.168.1.1/24), then press **Enter**.

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.)

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 any Ethernet port from 0/2 to 0/4 (bgroup0 interface in the Trust zone) on the device.

2. Ensure that your workstation is configured for DHCP or is statically configured with an IP address in the 192.168.1.0/24 subnet.

3. Start a Telnet client application to the IP address for the bgroup0 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 remove the timeout, enter **set console timeout 0**.

Default Device Settings

This section describes the default settings and operation of the SSG 20 device.

Table 5 shows the default zone bindings for ports on the devices.

Table 5: Default Physical Interface to Zone Bindings

Port Label	Interface	Zone
10/100 Ethernet ports:		
0/0	ethernet0/0	Untrust
0/1	ethernet0/1	DMZ
0/2	bgroup0 (ethernet0/2)	Trust
0/3	bgroup0 (ethernet0/3)	Trust
0/4	bgroup0 (ethernet0/4)	Trust
AUX	serial0/0	Null

Bridge groups (bgroups) let network users switch between wired and wireless traffic without having to reconfigure or restart their workstations. By default, the ethernet0/2 — ethernet0/4 interfaces, labeled as ports 0/2 — 0/4 on the device, are grouped together as the bgroup0 interface, have the IP address 192.168.1.1/24, and are bound to the Trust security zone. You can configure up to four bgroups.

You can change the default IP address on the bgroup0 interface to match the addresses on your LAN and WLAN. For configuring a wireless interface to a bgroup, see “Basic Wireless Configuration” on page 33.

NOTE: The bgroup interface does not work in Transparent mode when it contains a wireless interface.

For additional bgroup information and examples, refer to the *Concepts & Examples ScreenOS Reference Guide*.

Table 6 shows the default zone bindings for wireless and logical interfaces.

Table 6: Wireless and Logical Interface Bindings

SSG 20-WLAN	Interface	Zone
Wireless Interface		
Specifies a wireless interface, which is configurable to operate on 2.4G and/or 5G radio	wireless0/0 (default IP address is 192.168.2.1/24).	Trust
	wireless0/1-0/3.	Null
Logical Interfaces		
Layer-2 interface	vlan1 specifies the logical interfaces used for management and VPN traffic termination while the device is in Transparent mode.	-
Tunnel interfaces	tunnel.*n* specifies a logical tunnel interface. This interface is for VPN traffic.	-

There are no other default IP addresses configured on other Ethernet or wireless interfaces on a device; you need to assign IP addresses to the other interfaces, including the WAN interfaces.

Basic Device Configuration

The following sections describe the basic configuration tasks required to place the SSG 20 device in operation:

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 (netscreen) and password (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 in your network can manage the device if they know the admin name and password.

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 bgroup0 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 any of the bgroup0 ports on the device. 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 bgroup0): Enter the following, then click **OK**:

IP Address/Netmask: *ip_addr/mask*

CLI

set interface bgroup0 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.

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

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 CLI **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**:

IP Address/Netmask: 0.0.0.0/0.0.0.0
Next Hop
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 20 device is pre-configured with bridge group (bgroup) interfaces identified as bgroup0 through bgroup3. By default, the Ethernet interfaces ethernet0/2—ethernet0/4 are grouped together in bgroup0, which is bound to the Trust security zone.

Bgroups let you group multiple Ethernet and wireless 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.

NOTE: You can only bind wireless and Ethernet interfaces to bgroups.

To configure a bridge group with Ethernet and wireless interfaces:

WebUI

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

Edit (bgroup1) > Bind Port: Select **ethernet0/3**, **ethernet0/4**, and **wireless0/2**, then click **Apply**.

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

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

CLI

```
unset interface bgroup0 port ethernet0/3
unset interface bgroup0 port ethernet0/4
set interface bgroup1 port ethernet0/3
set interface bgroup1 port ethernet0/4
set interface bgroup1 port wireless0/2
set interface bgroup1 zone DMZ
set interface bgroup1 ip 10.0.0.1/24
save
```

If you want to bind an Ethernet or a wireless interface to a bgroup, you must first make sure that the Ethernet or wireless interface is in the Null security zone. Unsetting the Ethernet or wireless 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.

To unbind ethernet0/3 from bgroup0 and assign it to the Trust zone with a static IP address of 192.168.3.1/24:

WebUI

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

List > Edit (ethernet0/3): Enter the following, then click **Apply**:

Zone Name: Trust (select)
IP Address/Netmask: 192.168.3.1/24

CLI

```
unset interface bgroup0 port ethernet0/3
set interface ethernet0/3 zone trust
set interface ethernet0/3 ip 192.168.3.1/24
save
```

Backup Untrust Interface Configuration

The SSG 20 device lets you configure a backup interface for untrust failover. To set a backup interface for untrust failover, perform the following steps:

1. Set the backup interface in the Null security zone with the **unset interface** *interface* [**port** *interface*] command.

2. Bind the backup interface to the same security zone as the primary interface with the **set interface** *interface* **zone** *zone_name* command.

NOTE: The primary and backup interfaces must be in the same security zone. One primary interface has only one backup interface, and one backup interface has only one primary interface.

To set the ethernet0/4 interface as the backup interface to the ethernet0/0 interface:

WebUI

Network > Interfaces > Backup > Enter the following, then click **Apply**.

Primary: ethernet0/0
Backup: ethernet0/4
Type: track-ip (select)

CLI

```
unset interface bgroup0 port ethernet0/4
set interface ethernet0/4 zone untrust
set interface ethernet0/0 backup interface ethernet0/4 type track-ip
save
```

Basic Wireless Configuration

This section describes how to configure the wireless interface on the SSG 20-WLAN device. Wireless networks consist of names referred to as Service Set Identifiers (SSIDs). Specifying SSIDs allows you to have multiple wireless networks reside in the same location without interfering with each other. An SSID name can have a maximum of 32 characters. If a space is part of the SSID name string, then the string must be enclosed with quotation marks. Once the SSID name is set, more SSID attributes can be configured.To use the wireless local area network (WLAN) capabilities on the device, you must configure at least one SSID and bind it to a wireless interface.

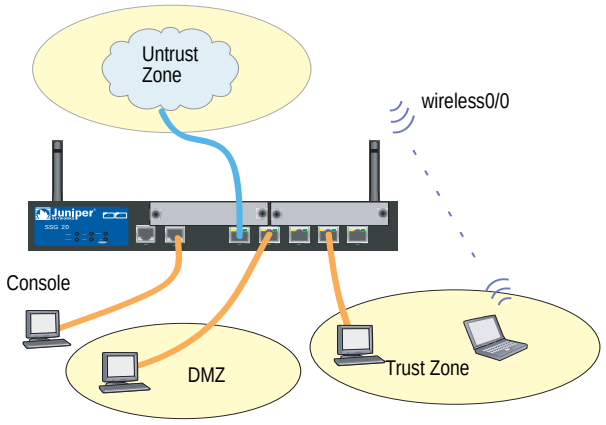
The SSG 20-WLAN device lets you create up to 16 SSIDs, but only 4 of them can be used simultaneously. You can configure the device to use the 4 SSIDs on either one of the transceivers or split the use on both (for example, 3 SSIDs assigned to WLAN 0 and 1 SSID assigned to WLAN 1.) Use the **set interface** *wireless_interface* **wlan** {0 | 1 | both} command to set the radio transceivers on the SSG 20-WLAN device.

Once you have set an SSID to the wireless0/0 interface, you can access the device using the default wireless0/0 interface IP address in the steps described in “Accessing the Device” on page 24. Figure 11 on page 34 shows the default configuration for the SSG 20-WLAN device.

NOTE: If you are operating the SSG 20-WLAN device in a country other than the United States, Japan, Canada, China, Taiwan, Korea, Israel, or Singapore, you must set the country code with the **set wlan country-code** CLI command or set it on the Wireless > General Settings WebUI page before a WLAN connection can be established. This command sets the selectable channel range and the transmit power level.

If your regional code is ETSI, you must set the correct country code that meets your local radio spectrum regulations.

Figure 11: Default SSG 20-WLAN Configuration



By default, the wireless0/0 interface is configured with the IP address 192.168.2.1/24. All wireless clients that need to connect to the Trust zone must have an IP address in the wireless subnetwork. You can also configure the device to use DHCP to automatically assign IP addresses in the 192.168.2.1/24 subnetwork to your devices.

By default, the wireless0/1 – wireless0/3 interfaces are bound to the Null zone and are not assigned IP addresses. If you want to use any other wireless interface, you must configure an IP address for it, assign an SSID to it, and bind it to a security zone. Table 7 shows the wireless authentication and encryption methods.

Table 7: Wireless Authentication and Encryption Options

Authentication	Encryption
Open	Allows any wireless client to access the device
Shared-key	WEP shared-key
WPA-PSK	AES/TKIP with pre-shared key
WPA	AES/TKIP with key from RADIUS server
WPA2-PSK	802.11i compliant with a pre-shared key
WPA2	802.11i compliant with a RADIUS server
WPA-Auto-PSK	Allows WPA and WPA2 type with pre-shared key
WPA-Auto	Allows WPA and WPA2 type with RADIUS server
802.1x	WEP with key from RADIUS server

Refer to the *Concepts & Examples ScreenOS Reference Guide* for configuration examples, SSID attributes, and CLI commands relating to wireless security configurations.

To configure a wireless interface for basic connectivity:

WebUI

1. Set the WLAN country code and IP address.

   Wireless > General Settings > Select the following, then click **Apply**:

   Country code: Select your code
   IP Address/Netmask: *ip_add/netmask*

2. Set the SSID.

   Wireless > SSID > New: Enter the following, then click **OK**:

   SSID:
   Authentication:
   Encryption:
   Wireless Interface Binding:

3. (Optional) set the WEP key.

   SSID > WEP Keys: Select the keyID, then click **Apply**.

4. Set the WLAN mode.

   Network > Interfaces > List > Edit (wireless interface): Select **Both** for the WLAN mode, then click **Apply**.

5. Activate wireless changes.

   Wireless > General Settings > Click **Activate Changes**.

CLI

1. Set the WLAN country code and IP address.

   set wlan country-code {*code_id*}
   set interface *wireless_interface* ip *ip_addr/netmask*

2. Set the SSID.

   set ssid name *name_str*
   set ssid *name_str* authentication *auth_type* encryption *encryption_type*
   set ssid *name_str* interface *interface*
   (optional) set ssid *name_str* key-id *number*

3. Set the WLAN mode.

   set interface *wireless_interface* wlan both

4. Activate wireless changes.

   save
   exec wlan reactivate

You can set an SSID to operate in the same subnet as the wired subnet. This action allows clients to work in either interface without having to reconnect in another subnet.

To set an Ethernet and a wireless interface to the same bridge-group interface:

WebUI

Network > Interfaces > List > Edit (*bgroup_name*) > Bind Port: Select the wireless and ethernet interfaces, then click **Apply**.

CLI

set interface *bgroup_name* port *wireless_interface*
set interface *bgroup_name* port *ethernet_interface*

NOTE: *Bgroup_name* can be bgroup0—bgroup3.

Ethernet_interface can be ethernet0/0—ethernet0/4.

Wireless_interface can be wireless0/0—wireless0/3.

If a wireless interface is configured, then you need to reactivate the WLAN with the **exec wlan reactivate** CLI command or click **Activate Changes** on the Wireless > General Settings WebUI page.

Mini-PIM Configuration

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

Basic Firewall Protections

The SSG 20 device is 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*.

The SSG 20 device provides 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 *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 38
- "Restarting the Device with the WebUI" on page 38

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 easiset 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 24.
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 24, 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 24.

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 20 device. It contains the following sections:

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.

Required Tools and Parts

To replace a component on the SSG 20 device, you must have the following tools and parts:

- Electrostatic bag or antistatic mat
- Electrostatic discharge (ESD) grounding wrist strap
- Number-2 Phillips screwdriver

Replacing Mini-Physical Interface Modules

Both SSG 20 models have two slots in the front panel for wide area network mini-physical interface modules (WAN mini-PIMs). mini-PIMs in SSG 20 devices can be installed and replaced. The device must be powered off before you can remove or install a mini-PIM.

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

Removing a Blank Faceplate

To maintain proper airflow through the SSG 20 device, blank faceplates should remain over slots that do not contain mini-PIMs. Do not remove a blank faceplate unless you are installing a mini-PIM in its empty slot.

To remove a blank faceplate:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface on which you intend to place the mini-PIM.
2. 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 SSG 20 device is disconnected from earth ground.
3. Unplug the power adapter from the device. Verify that the POWER LED is off.
4. Loosen and remove the screws on each side of the faceplate using a screwdriver.
5. Remove the faceplate.

Removing a Mini-PIM

Mini-PIMs are installed in the front panel of the SSG 20 device. A mini-PIM weighs less than 0.2 lb (106g).

To remove a mini-PIM:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface on which you intend to place the mini-PIM.
2. 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 SSG 20 device is disconnected from earth ground.
3. Unplug the power adapter from the device. Verify that the POWER LED is off.
4. Label the cables connected to the mini-PIM so that you can later reconnect each cable to the correct mini-PIM.
5. Disconnect the cables from the mini-PIM.

6. If necessary, arrange the cables to prevent them from dislodging or developing stress points.

7. Loosen and remove the screws on each side of the mini-PIM faceplate using a screwdriver.

8. Grasp the screws on each side of the mini-PIM faceplate and slide the mini-PIM out of the device. Place the mini-PIM in the electrostatic bag or on the antistatic mat.

Figure 12: Removing a Mini-PIM

9. If you are not reinstalling a mini-PIM into the empty slot, install a blank faceplate over the slot to maintain proper airflow.

Installing a Mini-PIM

To install a mini-PIM:

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 SSG 20 device is disconnected from earth ground.

2. Unplug the power adapter from the device. Verify that the POWER LED is off.

3. Grasp the screws on each side of the mini-PIM faceplate and align the notches in the connector at the rear of the mini-PIM with the notches in the mini-PIM slot in the SSG 20 device. Then slide the mini-PIM in until it seats firmly in the device.

Figure 13: Installing a Mini-PIM

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

4. Tighten the screws on each side of the mini-PIM faceplate using a 1/8-inch slotted screwdriver.
5. Insert the appropriate cables into the cable connectors on the mini-PIM.
6. If necessary, arrange the cables to prevent them from dislodging or developing stress points:
   a. Secure the cables so that they are not supporting their own weight as they hang to the floor.
   b. Place any excess cables out of the way in neatly coiled loops.
   c. Use fasteners to maintain the shape of the cable loops.
7. Unplug the power adapter from the device. Verify that the POWER LED glows steadily green after you press the power button.
8. Verify that the PIM status LED on the system dashboard glows steadily green to confirm that the mini-PIM is online.

Upgrading Memory

To upgrade the SSG 20 device from 128 MB to 256 MB of memory:

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. Unplug the AC cord from the power outlet.
3. Turn over the device so that its top is lying on a flat surface.
4. Use a phillips screwdriver to remove the screws from the memory-card cover. Keep the screws nearby for use when securing the cover later.
5. Remove the memory-card cover.

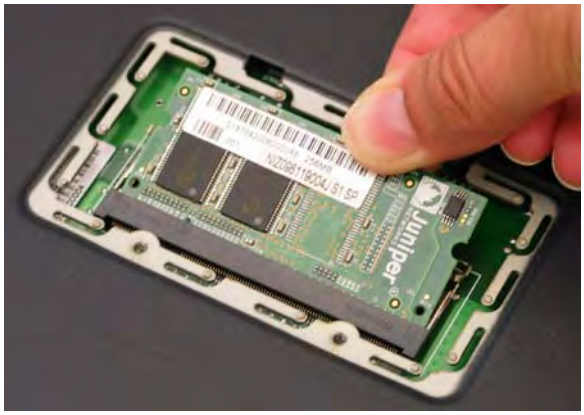
Figure 14: Bottom of Device

6. Release the 128 MB DIMM DRAM by pressing your thumbs outward on the locking tabs on each side of the module so that the tabs move away from the module.

Figure 15: Unlocking the Memory Module

7. Grip the long edge of the memory module and slide it out. Set it aside.

Figure 16: Removing Module Slots



8. Insert the 256 MB DIMM DRAM into the slot. Exerting even pressure with both thumbs upon the upper edge of the module, press the module downward until the locking tabs click into position.

Figure 17: Inserting the Memory Module

9. Place the memory-card cover over the slot.
10. Use the phillips screwdriver to tighten the screws, securing the cover to the device.

Appendix A
Specifications

This appendix provides general system specifications for the SSG 20 device. It contains the following sections:

Physical

Table 8 lists physical specifications for the SSG 20 device.

Table 8: SSG 20 Physical Specifications

Description	Value
Chassis dimensions	294 mm x 194.8 mm x 44 mm (11.5 inches x 7.7 inches x 2 inches)
Device weight	1.53 kg (3.3 lbs) without PIMs installed

Electrical

Table 9 lists electrical specifications for the SSG 20 device.

Table 9: SSG 20 Electrical Specifications

Item	Specification
DC input voltage	12V
DC system current rating	3 - 4.16 Amps

Environmental Tolerance

Table 10 lists environmental tolerance specifications for the SSG 20 device.

Table 10: SSG 20 Environmental Tolerance

Description	Value
Altitude	No performance degradation to 6,600 ft (2,000 m)
Relative humidity	Normal operation ensured in relative humidity range of 10 to 90 percent, noncondensing
Temperature	Normal operation ensured in temperature range of 32°F (0°C) to 104°F (40°C) Nonoperating storage temperature in shipping carton: -4°F (-20°C) to 158°F (70°C)

Certifications

Table 11 lists certifications for the SSG 20 device.

Table 11: SSG 20 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 (2000) Third Edition Safety of Information Technology Equipment IEC 60950-1 (1999) Third Edition Safety of Information Technology Equipment
EMC Emissions	FCC Part 15 Class B (USA) EN 55022 Class B (Europe) AS 3548 Class B (Australia) VCCI Class B (Japan)
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 EN-61000-4-11 Voltage Dips and Sags
ETSI	European Telecommunications Standards Institute (ETSI) EN-300386-2: Telecommunication Network Equipment. Electromagnetic Compatibility Requirements (equipment category Other than telecommunication centers)
T1 Interface	FCC Part 68 - TIA 968 Industry Canada CS-03 UL 60950-1 Applicable requirements for TNV circuit with outside plant lead connection

RoHS and WEEE

Juniper Networks products comply with the European Union's Waste Electrical and Electronic Equipment (WEEE) Directive and Restriction of Hazardous Substances (RoHS) Directive. These directives and other similar regulations from countries outside the European Union, China and Korea, relate to electronic waste management and the reduction or elimination of specific hazardous materials in electronic products.

For more information about RoHS and WEEE compliance, visit:

www.juniper.net/environmental

Connectors

Figure 18 shows the pin numbering of the RJ-45 connectors for the Console and AUX ports.

Figure 18: RJ-45 Connector Pin Numbering

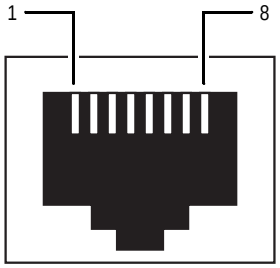


Table 12 lists the pinouts of the RJ-45 connectors for the Console and AUX ports.

Table 12: 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 19 shows the pin numbering of the connector on the DB-9 adapter.

Figure 19: DB-9 Female Connector

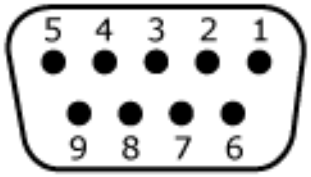


Table 13 lists the pinouts for the DB-9 adapter.

Table 13: 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

Appendix B

Initial Configuration Wizard

This appendix provides detailed information about the Initial Configuration Wizard (ICW) for the SSG 20 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

Figure 20: 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 NSM administrator, select **Yes**, select **Load Configlet from:**, browse to the file location, then click **Next**. The configlet sets up the device for you, so you don't need to use the following steps to configure the device.

If you want to bypass the ICW 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 ICW, 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 21: Administrator Login Window

3. WLAN Access Point Window

If you are using the device in the WORLD or ETSI regulatory domain, you must choose a country code. Select the appropriate options, then click **Next**.

Figure 22: Wireless Access Point Country Code Window

4. Physical Interface Window

On the interface-to-zone bindings screen, you set the interface to which you want to bind the Untrust security zone. Bgroup0 is prebound to the Trust security zone. Eth0/1 is bound to the DMZ security zone but is optional.

Figure 23: Physical Interface Window

After binding an interface to a zone, you can configure the interface. The configuration windows that are displayed after this point depend on which Mini-PIMs are installed in your security device. To continue configuring your device with the ICW, click **Next**.

5. ADSL2/2+ Interface Window

If you have the ADSL2/2 + Mini-PIM installed in your device, you can configure the adslx/0 interface using the following window.

NOTE: If you have two ADSL2/2 + Mini-PIMs installed on your device, you cannot configure the Multi-link feature with the ICW. To configure ML ADSL, refer to the *Concepts & Examples ScreenOS Reference Guide*.

Figure 24: ADSL Interface Configuration Window

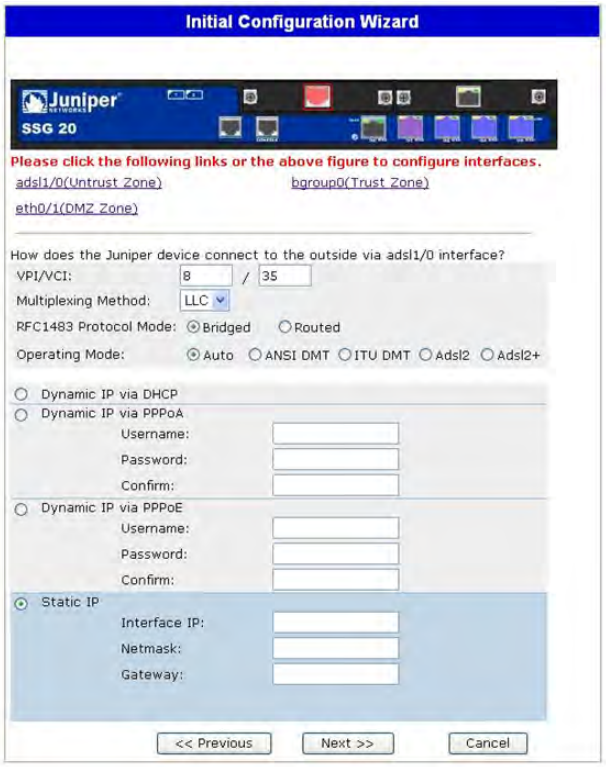


Table 14: Fields in ADSL Interface Configuration Window

Field	Description
Information from Service Provider:	
VPI/VCI	VPI/VCI values to identify the permanent virtual circuit.
Multiplexing Method	ATM multiplexing method (**LLC** is the default).
RFC1483 Protocol Mode	Protocol mode setting (**Bridged** is the default).
Operating Mode	Operating mode for the physical line (**Auto** is the default).
IP configuration settings	■ Select **Dynamic IP via DHCP** to enable the device to receive an IP address for the ADSL interface from a service provider. ■ Select **Dynamic IP via PPPoA** to enable the device to act as a PPPoA client. Enter the username and password assigned by the service provider. ■ Select **Dynamic IP via PPPoE** to enable the device to act as a PPPoE client. Enter the username and password assigned by the service provider. ■ Select **Static IP** to assign a unique and fixed IP address to the ADSL interface. Enter the interface IP address, netmask, and gateway (the gateway address is the IP address of the router port connected to the device).

If you do not know these settings, refer to the *Common Settings for Service Providers* document that came with the service provider device.

6. T1 Interface Windows

If you have the T1 Mini-PIM installed in your device and you selected the Frame Relay option, the following windows are displayed:

- T1 Physical Layer Tab Window
- T1 Frame Relay Tab Window

NOTE: If you have two T1 Mini-PIMs installed on your device and you select the Multi-link option, you will see two Physical Layer tabs.

Figure 25: T1 Physical Layer Tab Window

Table 15: Fields in T1 Physical Layer Tab Window

Field	Description
Clocking	Sets the transmit clock on the interface.
Line Buildout	Sets the distance at which an interface drives a line. Default setting is 0 - 132 feet.
Line Encoding	Sets the line encoding format on the interface: ■ Auto Mark Inversion ■ 8-bits zero suppression
Bye Encoding	Sets the byte encoding on the T1 interface to use 7 bits per byte or 8 bits per byte. Default is 8 bits per byte.
Frame Checksum	Sets the size of checksum. Default is **16**.
Framing Mode	Sets the framing format. Default is **Extended mode**.
Idle Cycles Flag	Sets the value that the interface transmits during idle cycles. Default setting is **0x7E**: ■ 0x7E (flags) ■ 0xFF (ones)
Start/End Flags	Sets the transmission of start and end flags to either filler or shared. The default is **filler**.
Invert Data checkbox	Enables inverted transmission of unused data bits.
Loopback Respond checkbox	Enables loopback on the T1 interface from the remote channel service unit (CSU).
Time Slots	Sets the use of time slots on a T1 interface. Default is **0**, all 24 time slots used.

Figure 26: T1 Frame Relay Tab Window

Table 16: Fields in T1 Frame Relay Tab Window

Field	Description
No-Keepalive checkbox	Enables no-keepalives.
Type	Sets the frame relay LMI type: ■ ANSI: American National Standards Institute supports data rates up to 8Mbps downstream and 1Mbps upstream. ■ ITU: International Telecommunications Union supports data rates of 6.144 Mbps downstream and 640 kbps upstream.
Interface Name	Sets the subinterface name.
Inverse ARP	Enables inverse Address Resolution Protocol for the subinterface.
Frame Relay DLCI	Assigns a data link connection identifier (DLCI) to the subinterface.
Interface IP	Sets the IP address for the subinterface.
Netmask	Sets the netmask for the subinterface.
Gateway	Sets the gateway address for the subinterface.

If you have the T1 Mini-PIM installed in your device and you selected the PPP option, the following additional windows are displayed:

- PPP Option with PPP Tab Window
- PPP Option with Peer User Tab Window

Figure 27: PPP Option with PPP Tab Window

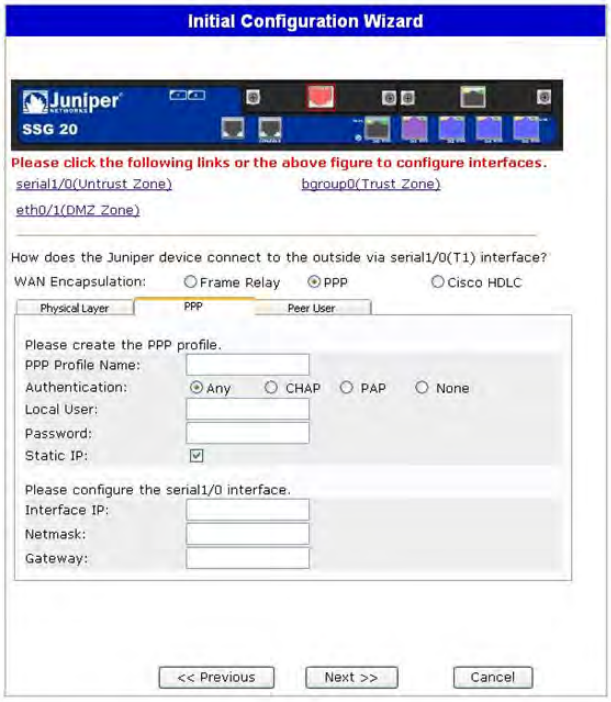


Table 17: Fields in PPP Option with PPP Tab Window

Field	Description
PPP Profile Name	Sets the name of the PPP profile
Authentication	Sets the authentication type
Local User	Sets the name of the local user
Password	Sets the password for the local user
Static IP checkbox	Enables a static IP address
Interface IP	Sets the serialx/0 interface IP address
Netmask	Sets the serialx/0 netmask
Gateway	Sets the serialx/0 gateway address

Figure 28: PPP Option with Peer User Tab Window

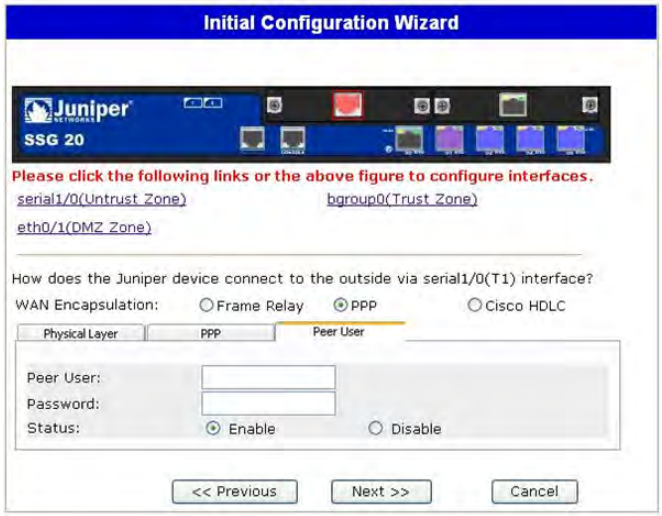


Table 18: Fields in PPP Option with Peer User Tab Window

Field	Description
Peer User	Sets the name of the peer user
Password	Sets the password for the peer user specified in the Peer User text field
Status	Enables or disables PPP

If you have the T1 Mini-PIM installed in your device and you selected the Cisco HDLC option, the following window is displayed:

Figure 29: Cisco HDLC Option with Cisco HDLC Tab Window

Table 19: Fields in Cisco HDLC Option with Cisco HDLC Tab Window

Field	Description
Interface IP	Sets the IP address for the T1 Cisco HDLC interface
Netmask	Sets the netmask for the T1 Cisco HDLC interface
Gateway	Sets the gateway address for the T1 Cisco HDLC interface

7. E1 Interface Windows

If you have the E1 Mini-PIM installed in your device and you selected the Frame Relay option, the following windows are displayed:

- E1 Physical Layer Tab Window
- E1 Frame Relay Tab Window

NOTE: If you have two E1 Mini-PIMs installed on your device and you select the Multi-link option, you will see two Physical Layer tabs.

Figure 30: E1 Physical Layer Tab Window

Table 20: Fields in E1 Physical Layer Tab Window

Field	Description
Clocking	Sets the transmit clock on the interface.
Frame Checksum	Sets the size of checksum. Default is **16**.
Framing Mode	Sets the framing format. Default is **without CRC4**.
Idle Cycles Flag	Sets the value that the interface transmits during idle cycles. Default setting is **0x7E**: ■ 0x7E (flags) ■ 0xFF (ones)
Start/End Flags	Sets the transmission of start and end flags to either filler or shared. The default is filler.
Invert Data checkbox	Enables inverted transmission of unused data bits.
Time Slots	Sets the use of time slots on a E1 interface. Default is **0**, all 32 time slots used.

Figure 31: E1 Frame Relay Tab Window

Table 21: Fields in E1 Frame Relay Tab Window

Field	Description
No-Keepalive checkbox	Enables no-keepalives.
Type	Sets the frame relay LMI type: ■ ANSI: American National Standards Institute supports data rates up to 8Mbps downstream and 1Mbps upstream. ■ ITU: International Telecommunications Union supports data rates of 6.144 Mbps downstream and 640 kbps upstream.
Interface Name	Sets the subinterface name.
Inverse ARP checkbox	Enables inverse Address Resolution Protocol (ARP) for the subinterface.
Frame Relay DLCI	Assigns a DLCI to the subinterface.

Field	Description
Interface IP	Sets the IP address for the subinterface
Netmask	Sets the netmask for the subinterface
Gateway	Sets the gateway address for the subinterface

To configure the E1 interface with PPP options, see “PPP Option with PPP Tab Window” on page 61.

To configure the E1 interface with the Cisco HDLC, see “Cisco HDLC Option with Cisco HDLC Tab Window” on page 62.

8. ISDN Interface Windows

If you have the ISDN Mini-PIM installed in your device, you can configure the bri*x*/0 (Untrust) interface using the following window.

NOTE: If you have two ISDN Mini-PIMs installed in your device and you selected the Multi-link option, you will see two Physical Layer tabs.

Figure 32: ISDN Physical Layer Tab Window

Table 22: Fields in ISDN Physical Layer Tab Window

Field	Description
Switch Type	Sets the service provider switch type: ■ att5e: At&T 5ESS ■ ntdms100: Nortel DMS 100 ■ ins-net: NTT INS-Net ■ etsi: European variants ■ ni1: National ISDN-1
SPID1	Service Provider ID, usually a seven-digit telephone number with some optional numbers. Only the DMS-100 and NI1 switch types require SPIDs. The DMS-100 switch type has two SPIDs assigned, one for each B-channel.
SPID2	Backup service provider ID.
TEI Negotiation	Specifies when to negotiate TEI, either at startup or on the first call. Typically this setting is used for ISDN service offerings in Europe and connections to DMS-100 switches that are designed to initiate TEI negotiation.
Calling Number	ISDN network billing number.
Sending Complete checkbox	Enables sending of complete information to outgoing setup message. Usually only used in Hong Kong and Taiwan.

You can select the bri1/0 interface to connect using dialer, multi-link dialer, leased line, or dial with BRI. Selecting neither, one, or both options displays a window similar to the following.

Figure 33: ISDN Connection Tab Window

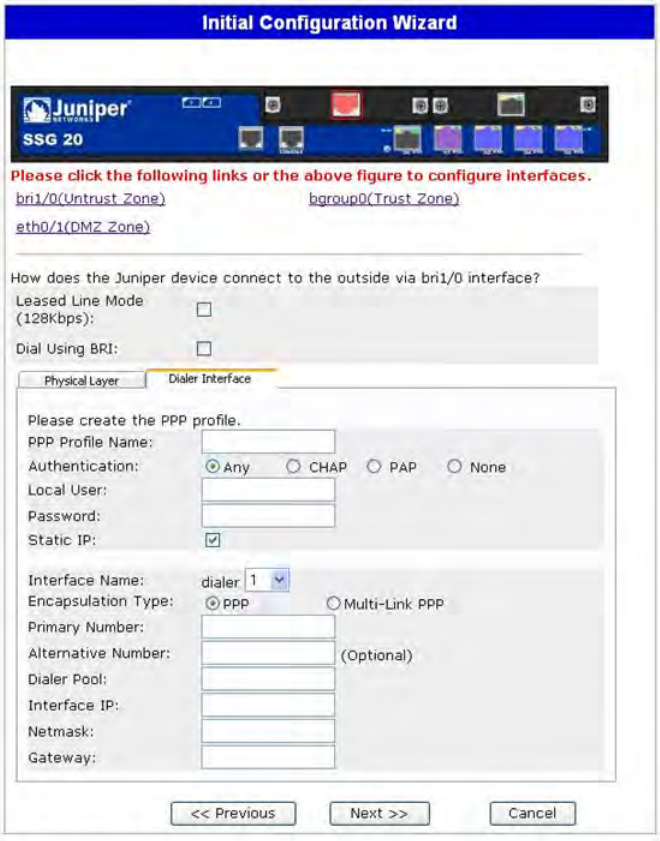


Table 23: Fields in ISDN Connection Tab Window

Field	Description
PPP Profile Name	Sets a PPP profile name to the ISDN interface.
Authentication	Sets the PPP authentication type: ■ Any ■ CHAP: Challenge Handshake Authentication Protocol ■ PAP: Password Authentication Protocol ■ None
Local User	Sets the local user.
Password	Sets the password for the local user.
Static IP checkbox	Enables a static IP address for the interface.
Interface IP	Sets the interface IP address.
Interface Name (Dialer only)	Sets the dialer interface name. Default is **dialer.1**.
Encapsulation Type	Sets the encapsulation type on the dialer and dialer using BRI interface. Default is **PPP**.
Primary Number	Sets the primary number for dialer and dialer using BRI interfaces.
Alternative Number	Sets the alternative (secondary) number to be used when the primary number cannot be used for connectivity.

Field	Description
Dialer Pool (Dialer only)	Sets the dialer pool name for the dialer interface.
Netmask	Sets the netmask.
Gateway	Sets the gateway address.

9. V.92 Modem Interface Window

If you have the V.92 Mini-PIM installed in your device, you can configure the serialx/0 (Modem) interface using the following window:

Figure 34: Modem Interface Window

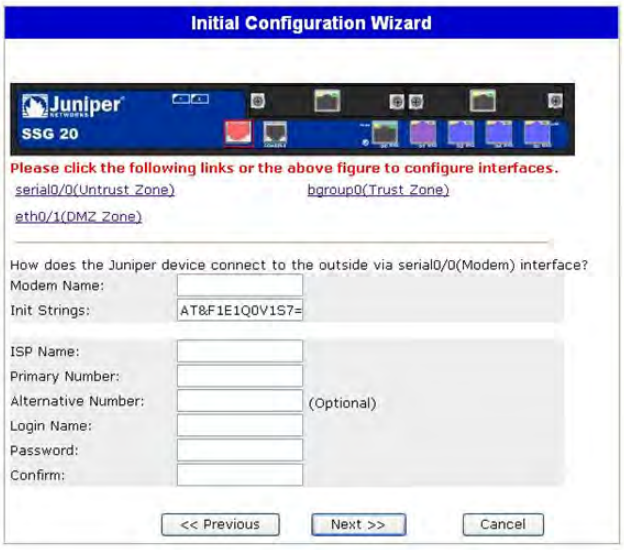


Table 24: Fields in Modem Interface Window

Field	Description
Modem Name	Sets the name for the modem interface
Init String	Sets the initialization string for the modem
ISP Name	Assigns a name to the service provider
Primary Number	Specifies the phone number to access the service provider
Alternative Number (optional)	Specifies an alternative phone number to access the service provider if the primary number does not connect
Login Name	Sets the login name for the service provider account
Password	Sets the password for the login name
Confirm	Confirms the password typed in the Password field

10. Eth0/0 Interface (Untrust Zone) Window

The eth0/0 interface can have a static or a dynamic IP address assigned via DHCP or PPPoE.

Figure 35: Eth0/0 Interface Window

Table 25: Fields in Eth0/0 Interface Window

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

11. Eth0/1 Interface (DMZ Zone) Window

The eth0/1 interface can have a static or a dynamic IP address assigned via DHCP.

Figure 36: Eth0/1 Interface Window

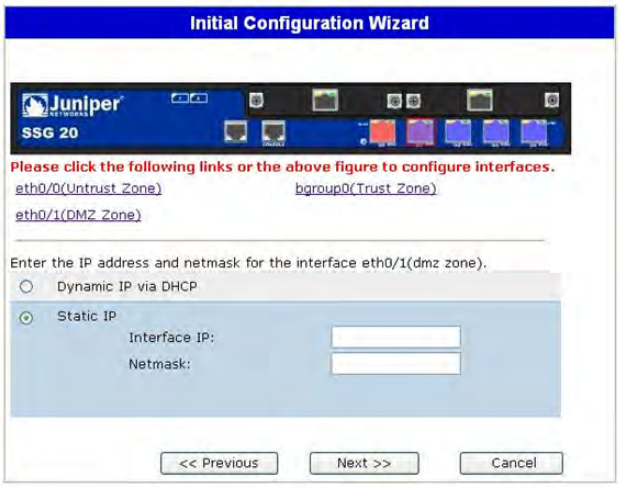


Table 26: Fields in Eth0/1 Interface Window

Field	Description
Dynamic IP via DHCP	Enables the device to receive an IP address for the DMZ interface from a service provider.
Static IP	Assigns a unique and fixed IP address to the DMZ interface. Enter the DMZ interface IP and netmask.

12. Bgroup0 Interface (Trust Zone) Window

The bgroup0 interface can have a static or a dynamic IP address assigned via DHCP.

The default interface IP address is **192.168.1.1** with a netmask of **255.255.255.0** or **24**.

Figure 37: Bgroup0 Interface Window

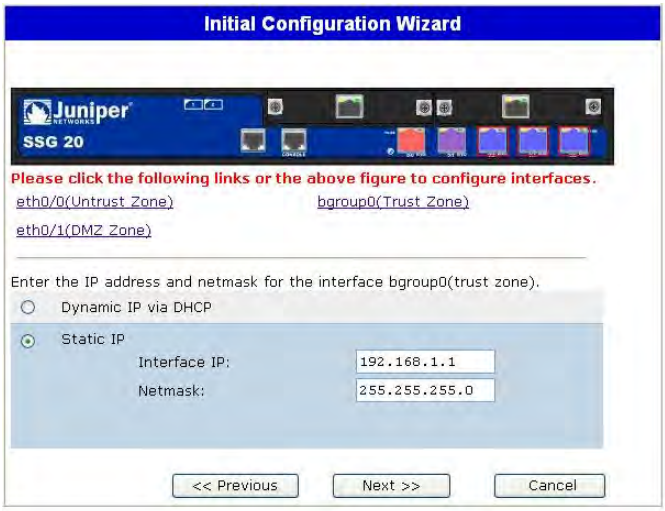


Table 27: Fields in Bgroup0 Interface Window

Field	Description
Dynamic IP via DHCP	Enables the device to receive an IP address for the Trust zone interface from a service provider.
Static IP	Assigns a unique and fixed IP address to the Trust zone interface. Enter the Trust zone interface IP address and netmask.

13. Wireless0/0 Interface (Trust Zone) Window

If you are configuring the SSG 20-WLAN device, you must set a Service Set Identifier (SSID) before the wireless0/0 interface can be activated. For detailed instructions about configuring your wireless interface(s), refer to the *Concepts & Examples ScreenOS Reference Guide*.

Figure 38: Wireless0/0 Interface Window

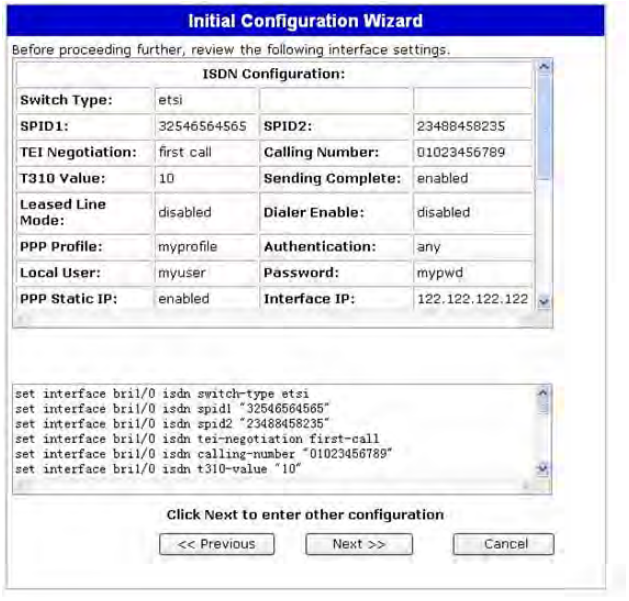
Table 28: Fields in Wireless0/0 Interface Window

Field	Description
Wlan Mode	Sets the WLAN radio mode: ■ 5G (802.11a). ■ 2.4G (802.11b/g). ■ Both (802.11a/b/g).
SSID	Sets the SSID name.
Authentication and Encryption	Sets the WLAN interface authentication and encryption: ■ **Open** authentication, the default, allows anyone to access the device. There is no encryption for this authentication option. ■ **WPA Pre-Shared Key** authentication sets the Pre-Shared Key (PSK) or passphrase that must be entered when accessing a wireless connection. You can choose to enter a HEX or an ASCII value for the PSK. A HEX PSK must be a 256-bit (64-text character) HEX value. An ASCII passphrase must be 8 to 63 text characters. You must select Temporal Key Integrity Protocol (**TKIP**) or Advanced Encryption Standard (**AES**) as the encryption type for this option, or select **Auto** to allow either option. ■ WPA2 Pre-Shared Key. ■ WPA Auto Pre-Shared Key.
Interface IP	Sets the WLAN interface IP address.
Netmask	Sets the WLAN interface netmask.

14. Interface Summary Window

After you have configured the WAN interfaces, you will see the Interface Summary window.

Figure 39: Interface Summary Window

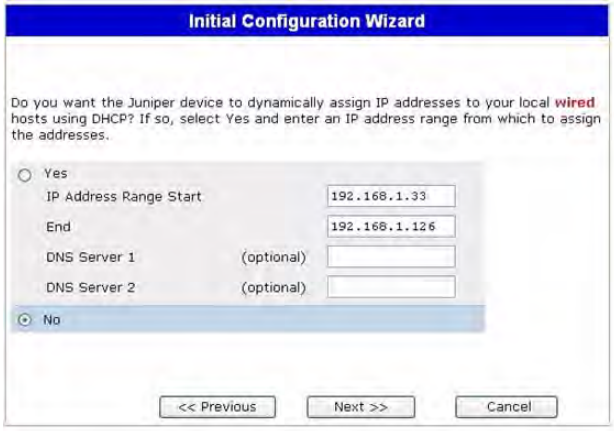


Check your interface configuration, then click **Next** when ready to proceed. The Physical Ethernet DHCP Interface window appears.

15. 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**.

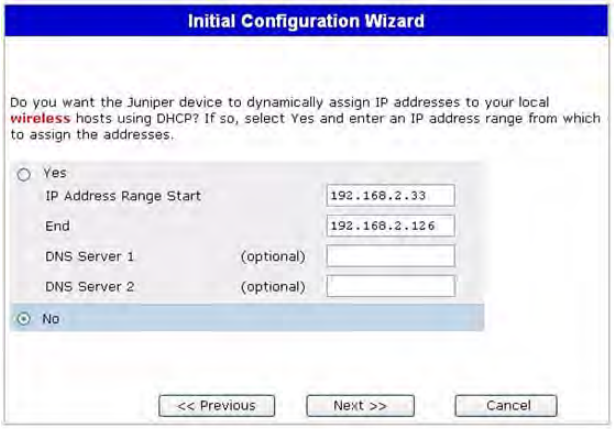
Figure 40: Physical Ethernet DHCP Interface Window



16. Wireless DHCP Interface Window

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

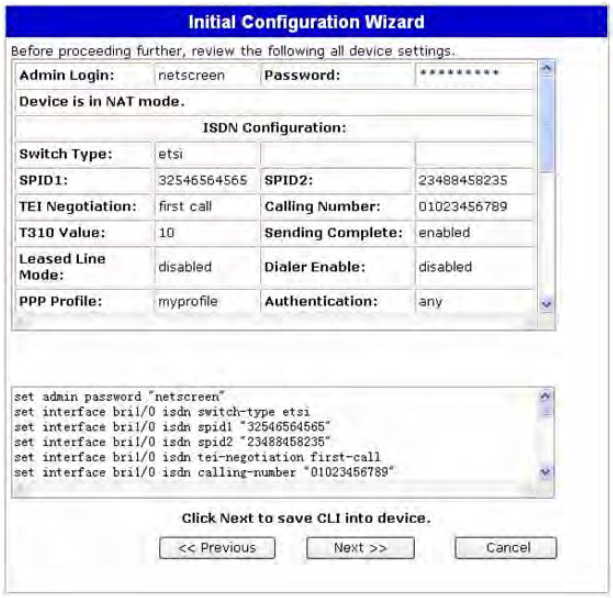
Figure 41: Wireless DHCP Interface Window



17. Confirmation Window

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

Figure 42: Confirmation Window



After the device restarts with the saved system configuration, the WebUI login prompt appears. For information on how to access the device using the WebUI, refer to “Using the WebUI” on page 26.

Appendix C

Country Code and Channel Information

This appendix lists information that might affect your deployment of a wireless LAN (WLAN). The information in this appendix applies only to devices in the world regulatory domain. The appendix contains the following sections:

Country Codes

For the most recent information on country codes for the SSG 5 and SSG 20, go to http://www.juniper.net/products/integrated/dsheet/800003.pdf

Wireless Channels

Table 29: Allowed Channels for All Countries (Sheet 1 of 2)

Country	Channel	Country	Channel
ALBANIA	1-13	LEBANON	1-13
ALGERIA	1-13	LIECHTENSTEIN	1-13
ARMENIA	1-13	LITHUANIA	1-13
AUSTRALIA	1-13	LUXEMBOURG	1-13
AUSTRIA	1-13	MACAU	1-13
AZERBAIJAN	1-13	MACEDONIA	1-13
BAHRAIN	1-13	MEXICO	1-11
BELARUS	1-13	MONACO	1-13
BELGIUM	1-13	MOROCCO	1-13
BELIZE	1-13	NETHERLANDS	1-13
BOLVIA	1-13	NEW ZEALAND	1-13
BRUNEI DARUSSALAM	1-13	NORTH KOREA	1-13
BULGARIA	1-13	NORWAY	1-13
CANADA	1-11	OMAN	1-13
CHINA	1-13	PAKISTAN	1-13
COLOMBIA	1-11	PANAMA	1-11

Table 29: Allowed Channels for All Countries (Sheet 2 of 2)

Country	Channel	Country	Channel
COSTA RICA	1-13	PERU	1-13
CROATIA	1-13	PHILIPPINES	1-13
CYPRUS	1-13	POLAND	1-13
DENMARK	1-13	PORTUGAL	1-13
DOMINICAN REPUBLIC	1-11	PUERTORICO	1-11
EGYPT	1-13	QATAR	1-13
EL SALVADOR	1-13	ROMANIA	1-13
ESTONIA	1-13	RUSSIA	1-13
FINLAND	1-13	SAUDIARABIA	1-13
FRANCE	1-13	SINGAPORE	1-13
FRANCE_RES	1-13	SLOVAK REPUBLIC	1-13
GEORGIA	1-13	SLOVENIA	1-13
GERMANY	1-13	SOUTH AFRICA	1-13
GREECE	1-13	SPAIN	1-13
GUATEMALA	1-11	SWEDEN	1-13
HONDURAS	1-13	SWITZERLAND	1-13
HONG KONG	1-13	SYRIA	1-13
HUNGARY	1-13	TAIWAN	1-13
ICELAND	1-13	THAILAND	1-13
INDIA	1-13	TRINIDAD & TOBAGO	1-13
INDONESIA	1-13	TUNISIA	1-13
IRAN	1-13	TURKEY	1-13
IRELAND	1-13	UKRAINE	1-13
ISRAEL	1-13	UNITED ARAB EMIRATES	1-13
ITALY	1-13	UNITED KINGDOM	1-13
JAPAN	1-13	UNITED STATES	1-11
JORDAN	1-13	URUGUAY	1-13
KAZAKHSTAN	1-13	UZBEKISTAN	1-11
KOREA REPUBLIC	1-13	VENEZUELA	1-13
KOREA REPUBLIC2	1-13	VIET NAM	1-13
KUWAIT	1-13	YEMEN	1-13
LATVIA	1-13	ZIMBABWE	1-13

Index