



## **Security Products**

# **Secure Services Gateway (SSG) 20 Hardware Installation and Configuration Guide- Beta3**

*ScreenOS Version 5.4.0*

### **Juniper Networks, Inc.**

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

**[www.juniper.net](http://www.juniper.net)**

1-888-314-JTAC ☐

(1-888-314-5822 - toll free in U.S., Canada, and Mexico) ☐

or go to the link to request service ☐

<http://www.juniper.net/support/requesting-support.html> ☐

## Copyright Notice

Copyright © 2006 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo 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 B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Network's 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.

- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

- This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter

□

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.

□

Writer: Carrie Nowocin

Editor: Lisa Eldridge

DGT Warning:

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備

1. 本機限在不干擾合法電台與不受被干擾保障條件下於室內使用
2. 為減少電磁波干擾，請妥適使用

# Table of Contents

	<b>About This Guide</b>	<b>vii</b>
	Organization .....	vii
	WebUI Conventions .....	viii
	CLI Conventions .....	viii
	Obtaining Documentation and Technical Support .....	ix
<b>Chapter 1</b>	<b>Hardware Overview</b>	<b>1</b>
	Port and Power Connectors .....	2
	Front Panel .....	3
	System Status LEDs .....	3
	Port Descriptions .....	5
	Ethernet Ports .....	5
	Console Port .....	5
	AUX Port .....	5
	Mini Physical Interface Module Port Descriptions .....	6
	Back Panel .....	8
	Power Adapter .....	8
	Radio Transceiver .....	8
	Grounding Lug .....	8
	Antennae Types .....	9
	Universal Serial Bus (USB) Host Module .....	9
<b>Chapter 2</b>	<b>Installing and Connecting the Device</b>	<b>11</b>
	Before You Begin .....	11
	Equipment Rack Installation .....	12
	Connecting the Interface Cable to a Device .....	12
	Connecting the Power .....	13
	Connect the Device to a Network .....	13
	Connect an SSG 20 Device to an Untrusted Network .....	13
	Connecting Ethernet Ports .....	13
	Connecting Serial (AUX/Console) Ports .....	13
	Connect an SSG Device to an Untrusted Network .....	14
	Connect Mini PIMs to an Untrusted Network .....	14
	Connecting Other Mini PIMs .....	15
	Connect the Device to an Internal Network or a Workstation .....	16
	Connecting Ethernet Ports .....	16
	Connecting the Wireless Antennae .....	16
<b>Chapter 3</b>	<b>Configure the Device</b>	<b>17</b>
	Access the Device .....	18
	Using a Console Connection .....	18
	Using the WebUI .....	19

Using Telnet .....	20
Default Device Settings .....	21
Basic Device Configuration .....	23
Changing the Root Admin Name and Password .....	23
Setting the Date and Time .....	24
Bridge Group Interfaces .....	24
Administrative Access .....	25
Management Services .....	25
Host and Domain Name .....	25
Default Route .....	26
Management Interface Address .....	26
Backup Untrust Interface Configuration .....	26
Wireless Configuration .....	27
Wireless Network Configuration .....	28
Authentication and Encryption .....	30
Mini PIM Configuration .....	30
Asymmetrical DSL (ADSL) 2/2 + Interface .....	30
Virtual Circuits to an ADSL2/2 + Interface .....	31
VPI/VCI and Multiplexing Method .....	32
PPPoE or PPPoA .....	32
Static IP Address and Netmask .....	33
The ISDN Interface .....	34
The T1 Interface .....	35
The E1 Interface .....	36
The V.92 Modem Interface .....	37
Basic Firewall Protections .....	37
Verify External Connectivity .....	38
Reset the Device to Factory Defaults .....	38
The Reset Pinhole .....	38
<b>Chapter 4    Servicing the Device</b> .....	<b>41</b>
Tools and Parts Required .....	41
Replacing a Physical Interface Module .....	41
Removing a Blank Faceplate .....	42
Removing a Mini PIM .....	42
Installing a Mini PIM .....	43
Memory Upgrade .....	44
<b>Appendix A    Specifications</b> .....	<b>A-I</b>
SSG 20 Physical Specifications .....	I
Electrical Specification .....	I
Environmental .....	II
Certifications .....	II
Safety .....	II
EMC (Emissions) .....	II
EMC Immunity .....	II
European Telecommunications Standards Institute (ETSI) .....	III
T1 Interface .....	III
Connectors .....	III
<b>Appendix A    Initial Configuration Wizard</b> .....	<b>A-I</b>
Using the Initial Configuration Wizard .....	I

**Index.....IX-1**



# 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 Ethernet only
- SSG 20-WLAN which has four integrated wireless interfaces.

Both of the SSG 20 devices support auxiliary (AUX), universal storage bus (USB) storage, and two mini physical interface module (PIM) slots that can hold any of the mini PIMs. The devices also provide protocol conversions between local area networks (LANs) and wide area networks (WANs).

## Organization

---

This document contains the following chapters:

Chapter 1, “Hardware Overview,” describes the chassis and components of an SSG 20 device.

Chapter 2, “Installing and Connecting the Device,” describes how to install an SSG 20 device in a standard 19-inch equipment rack and how to connect cables and power to the device.

Chapter 3, “Configure the Device,” describes how to configure and manage an SSG 20 device and how to perform some basic configuration tasks.

Chapter 4, “Servicing the Device,” describes service and maintenance procedures for an SSG 20 device.

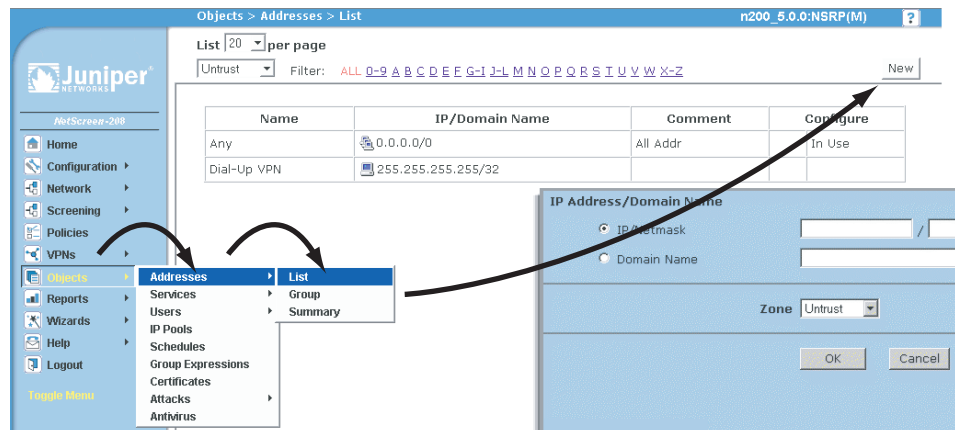
Appendix A, “Specifications,” provides general system specifications for an SSG 20 device.

Appendix B, “Initial Configuration Wizard,” describes the Initial Configuration Wizard steps.

## WebUI Conventions

A chevron ( > ) shows the navigational sequence through the WebUI, which you follow by clicking menu options and links. The following figure shows the following path to the address configuration dialog box—Objects > Addresses > List > New:

**Figure 1: WebUI Navigation**



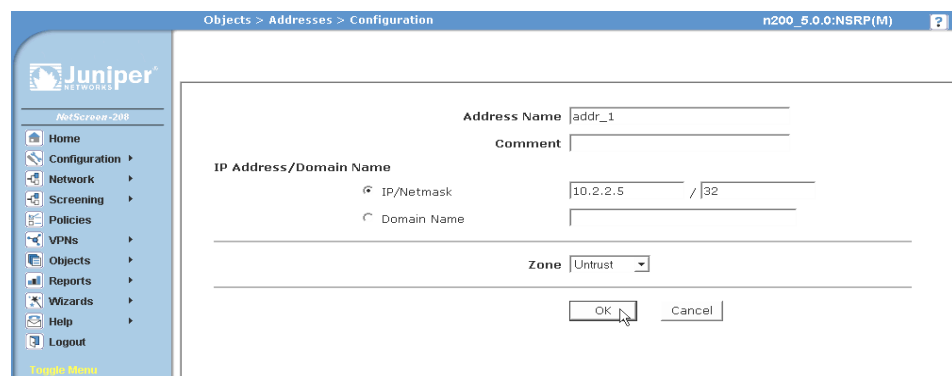
To perform a task with the WebUI, you first navigate to the appropriate dialog box, where you then define objects and set parameters. The set of instructions for each task is divided into navigational path and configuration settings:

The next figure lists the path to the address configuration dialog box with the following sample configuration settings:

Objects > 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

**Figure 2: Navigational Path and Configuration Settings**



## CLI Conventions

The following conventions are used to present the syntax of CLI commands in examples and in text.



In examples:

- 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:

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

means “set the management options for the ethernet1, the ethernet2, *or* the ethernet3 interface.”

- Variables are in *italic* type:

```
set admin user name1 password xyz
```

In text:

- Commands are in **boldface** type.
- Variables are in *italic* type.

---

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

---

## Obtaining Documentation and Technical Support

---

To obtain technical documentation for any Juniper Networks product, visit [www.juniper.net/techpubs/](http://www.juniper.net/techpubs/).

For technical support, open a support case using the Case Manager link at <http://www.juniper.net/support/> or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).

If you find any errors or omissions in this document, please contact us at the email address below:

[techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net)



## Chapter 1

# Hardware Overview

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

- “Port and Power Connectors” on this page
- “Front Panel” on page 3
- “Back Panel” on page 8

## Port and Power Connectors

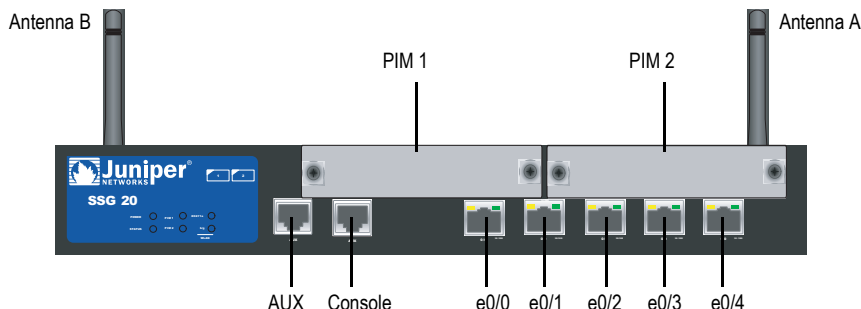


Table 1 shows the ports and power connectors on an SSG 20 device.

**Table 1: SSG 20 Port and Power Connectors**

Port	Description	Connector	Speed/Protocol
Ports 0/0-0/4	Enables direct connections to workstations or a LAN connection through a switch or hub. This connection also allows you to manage the device through a Telnet session or the WebUI.	RJ-45	10/100 Mbps Ethernet Autosensing duplex and auto MDI/MDIX
USB	Enables a 1.1 USB connection with the system.	N/A	12M (full speed) or 1.5M (low speed)
Console	Enables a serial connection with the system. Used for terminal-emulation connectivity to launch Command Line Interface (CLI) sessions.	RJ-45	9600 bps/ RS-232C serial
AUX	Enables a backup serial Internet connection through an external modem.	RJ-45	9600 bps — 115 Kbps/ RS-232C serial
Mini PIM			
ADSL 2/2 +	Enables an Internet connection through an ADSL data link.	RJ-11 (Annex A) RJ-45 (Annex B)	ANSI T1.413 Issue 2 (Annex A only) ITU G.992.1 (G.dmt) ITU G.992.2 (G.lite) (Annex A only) ITU G.992.3 (ADSL2) ITU G.992.5 (ADSL2 +)
V.92 Modem	Enables a primary or backup Internet or untrusted network connection to an Internet Service Provider (ISP).	RJ-11	9600 bps — 115 Kbps/ RS-232 Serial autosensing duplex and polarity
T1	Enables a connection to the T1 line to the untrusted network.	RJ-45	
E1	Enables a connection to the E1 line to the untrusted network.	RJ-45	
ISDN	Enables the ISDN line to be used as the untrust or backup interface.	RJ-45	B-channels at 64 Kbps
Antenna A & B (SSG 20-WLAN)	Enables a direct connection to workstations in the vicinity of a wireless radio connection.	RPSMA	802.11a (54 Mbps on 5GHz radio band) 802.11b (11 Mbps on 2.4GHz radio band) 802.11g (54 Mbps on 2.4GHz radio band) 802.11 superG (108 Mbps on 2.4GHz radio band)

## Front Panel

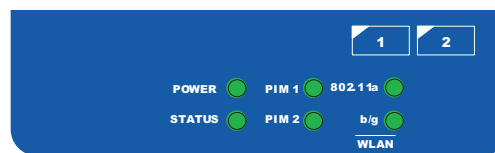
This section describes the following elements on the front panel of an SSG 20 device:

- System Status LEDs
- Port Descriptions
- Mini Physical Interface Module Port Descriptions

### System Status LEDs

The system status LEDs display information about critical device functions. Figure 1 illustrates the position of each status LED on the system dashboard. The WLAN LEDs are only present on the SSG 20-WLAN device.

**Figure 1: Status LED**



When the system 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 2 minutes to complete. If you want to turn the system off and on again, we recommend waiting a few seconds between shutting it down and powering it back up. Table 2 provides the name, color, status, and description of each system status LED.

**Table 2: LED Descriptions**

Name	Color	Status	Description
POWER	Green	On steadily	Indicates that the system is receiving power
		Off	Indicates that the system 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 system is booting up or performing diagnostics
		Blinking	Indicates that the device is operating normally
	Red	Blinking	Indicates that there was 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 not operational

<b>Name</b>	<b>Color</b>	<b>Status</b>	<b>Description</b>
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 not operational
WLAN			
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

## Port Descriptions

This section explains the purpose and function of the following:

- Ethernet Ports on page 5
- Console Port on page 5
- AUX Port on page 5

### Ethernet Ports

Five 10/100 Ethernet ports provide LAN connections to hubs, switches, local servers, and workstations. You can also designate an Ethernet port for management traffic. The ports are labeled **0/0** through **0/4**. For the default zone bindings for each Ethernet port, see “Default Device Settings” on page 21.

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 named **ethernet0/0** through **ethernet0/4**.

Figure 2 displays the location of the LEDs on each Ethernet port.

**Figure 2: Activity Link LEDs**

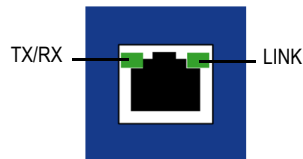


Table 3 describes the Ethernet port LEDs.

**Table 3: LAN Port LEDs**

Name	Color	Status	Description
LINK	Green	On steadily	Port is online
		Off	Port is offline
TX/RX	Green	Blinking	Traffic is passing through. The baud rate is proportional to the link activity.
		Off	Port might be on but is not receiving data

### Console Port

The Console port is an RJ-45 serial port wired as DCE that can be used for local administration. An RJ-45 to DB-9 adapter is supplied.

See “Connectors” on page III for the RJ-45 connector pinouts.

### 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.

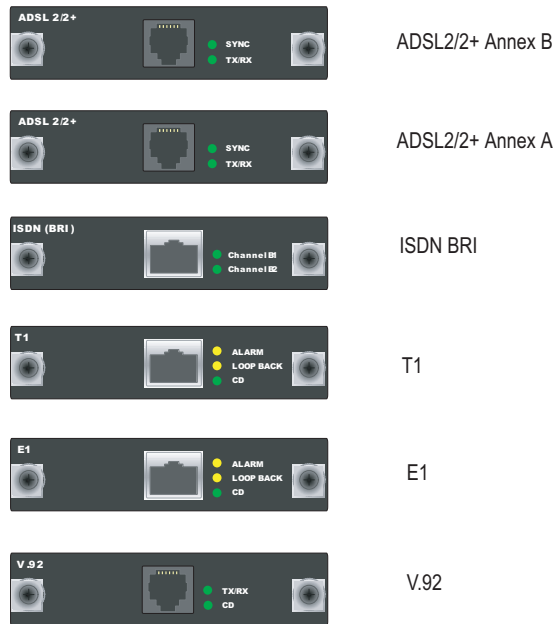
See “Connectors” on page III for the RJ-45 connector pinouts.

### Mini Physical Interface Module Port Descriptions

Each mini physical interface module (PIM) supported on a device has the following components:

- One cable connector port—Accepts a network media connector. Figure 3 shows the available mini PIMs. You can install up to two mini PIMs in a device.

**Figure 3: Mini PIMs on the SSG 20**



- Two to three status LEDs—Indicates port status. Table 4 describes the meaning of the LED states.



**Table 4: Mini PIM LED States on the SSG 20**

Type	Name	Color	State	Description
ADSL 2/2 + (Annex A and B)	SYNC	Green	On steadily	Indicates that the ADSL interface is trained
			Blinking	Indicates training is in progress
			Off	Interface is idle
	TX/RX	Green	Blinking	Indicates that traffic is passing through
			Off	Indicates that no traffic passing through
	ISDN (BRI)	CH B1	Green	On steadily
Off				Indicates that B-Channel 1 is not active
CH B2		Green	On steadily	Indicates that B-Channel 2 is active
			Off	Indicates that B-Channel 2 is not active
T1/E1	ALARM	Yellow	On steadily	Indicates that there is a local or remote alarm; device has detected a failure
			Off	Indicates that there are no alarms or failures
	LOOP BACK	Yellow	On steadily	Indicates that a loopback or line state is detected
			Off	Indicates that the loopback is not active
	CARRIER DETECT	Green	On steadily	Indicates a carrier was detected and the internal DSU/CSU in the mini PIM is communicating with another DSU/CSU
			Off	Indicates that carrier detect is not active
V.92	CD	Green	On steadily	Indicates that the link is active
			Off	Indicates that the serial interface is not in service
	TX/RX	Green	Blinking	Indicates that traffic is passing through
			Off	Indicates that no traffic is passing through

---

**NOTE:** Mini PIMs are not hot-swappable. They must be installed in the front panel slots before the system is booted up.

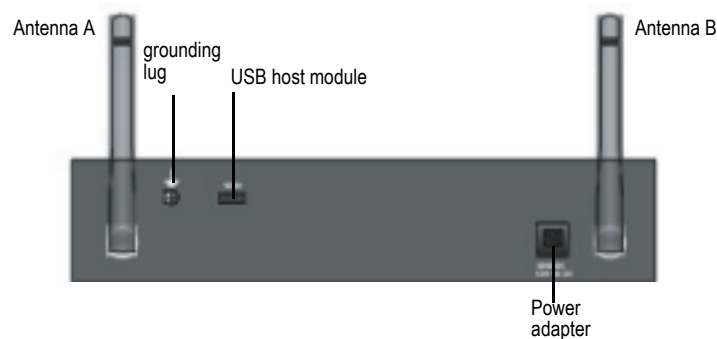
---

## Back Panel

This section describes the back panel of an SSG 20 device:

- “Power Adapter” on this page
- “Radio Transceiver,” on this page
- “Grounding Lug,” on this page
- “Antennae Types” on page 9
- “Universal Serial Bus (USB) Host Module” on page 9

**Figure 4: Back Panel of an SSG Device**



### Power Adapter

The POWER LED on the front panel of a device either glows green or is off. Green indicates correct function, and off indicates power adapter failure.

### Radio Transceiver

The SSG 20-WLAN contains two wireless connectivity radio transceivers, which support 802.11 a/b/g standards. The first transceiver (WLAN 0) uses the 2.4 GHz radio band, which supports the 802.11b standard at 11 Mbps, the 802.11g standard at 54 Mbps, and 802.11 SuperG standard at 108 Mbps. The second radio transceiver (WLAN 1) uses the 5 GHz radio band, which supports the 802.11a standard at 54 Mbps. The two radio transceivers can work simultaneously. For information on configuring the wireless radio band, see “*Wireless Network Configuration*” on page 28.

### Grounding Lug

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

To ground the device before connecting power, you 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 omnidirectional coverage and a fairly uniform level of signal strength within the area of coverage and are suitable for most installations. This type of antennae are 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 well suited for such places as hallways and outer walls (with the antenna facing inward).

## Universal Serial Bus (USB) Host Module

The slot labeled USB on the back panel of an SSG 20 device implements a host-only USB 1.1 host module for a USB device adapter or USB flash key, as defined in the *CompactFlash Specification* published by the CompactFlash Association. When the USB storage device is installed and configured, it automatically acts as a secondary storage device.

The USB host module allows file transfers, such as device configurations, user certifications, and update version images between an external USB flash key and the internal flash storage located in the security device. The USB host module supports USB 2.0 specification at either low-speed (1.5M) or full-speed (12M) file transfer.

To use a USB flash key to transfer files between the device, perform the following steps:

1. Insert the USB flash key into the USB host module on the security device.
2. Save the files from the USB flash key to the internal flash storage on the device with the **save { software | config | image-key } from usb filename to flash** CLI command.
3. Before removing the USB flash key, stop the host module with the **exec usb-device stop** CLI command.
4. It is now safe to remove the USB flash key.

If you want to delete a file from the USB flash key, use the **delete file usb:/filename** CLI command.

If you want to view the saved file information on the USB flash key or internal flash storage, use the **get file info** CLI command.



## Chapter 2

# Installing and Connecting the Device

This chapter describes how to install an SSG 20 device in a standard 19-inch equipment rack and connect cables and power to the device. Topics in this chapter include:

- “Before You Begin” on this page
- “Equipment Rack Installation” on page 12
- “Connecting the Interface Cable to a Device” on page 12
- “Connecting the Power” on page 13
- “Connect the Device to a Network” on page 13

---

**NOTE:** For safety warnings and instructions, please refer to the *Juniper Networks Security Products Safety Guide*. Before working on any equipment, you should be aware of the hazards involved with electrical circuitry and be familiar with 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 system operation.



**WARNING:** To prevent abuse and intrusion by unauthorized personnel, install an 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 that the room temperature does not exceed 104 × F (40 × C).

- Do not place the device in an equipment rack frame that blocks an intake or exhaust port. Ensure that enclosed racks have fans and louvered sides.
- Correct these hazardous conditions before any installation: moist or wet floors, leaks, ungrounded or frayed power cables, or missing safety grounds.

## Equipment Rack Installation

---

You can front-mount an SSG 20 device into a standard 19-inch equipment rack. The device is shipped with mounting brackets installed.

To front-mount an SSG 20 device, you need a number 2 phillips screwdriver (not provided) and four screws that are compatible with the equipment rack (not provided).

To install an SSG 20 device onto a rack:

1. Align the rack mount ears to the device.
2. Place the screws in the holes and use a phillips screwdriver to secure them.
3. Mount the device on the rack with the provided screws.
4. Plug the power supply into the power outlet.

## Connecting the Interface Cable to a Device

---

To connect the interface cable to a device, perform the following steps:

1. Have ready a length of the type of cable used by the interface.
2. Insert the cable connector into the cable-connector port on the interface faceplate.
3. Arrange the cable as follows to prevent it from dislodging or developing stress points:
  - a. Secure the cable so that it is not supporting its own weight as it hangs to the floor.
  - b. Place any excess cable out of the way in a neatly coiled loop.
  - c. Use fasteners to maintain the shape of the cable loops.

## Connecting the Power

---

To connect the power to a device, perform the following steps:

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



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

---

## Connect the Device to a Network

---

An SSG 20 device provides firewall and general security for networks when it is placed between internal networks and the untrusted network. This section describes the following:

- Connecting the device to an untrusted network
- Connecting the device mini PIMs to an untrusted Network
- Connecting the device to an internal network or workstation

### Connect an SSG 20 Device to an Untrusted Network

You can connect your SSG 20 device to the untrusted network in one of the following ways:

- Connecting Ethernet Ports
- Connecting Serial (AUX/Console) Ports

#### Connecting Ethernet Ports

To establish a high-speed connection, connect the provided Ethernet cable from the Ethernet port marked 0/0 on an SSG 20 device to the external router. This Ethernet port (0/0) is assigned to the ethernet0/0 interface, which is by default bound to the Untrust security zone. The device autosenses the correct speed, duplex, and MDI/MDIX settings.

#### Connecting Serial (AUX/Console) Ports

You can connect to the untrusted network with an RJ-45 straight through serial cable and external modem.



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

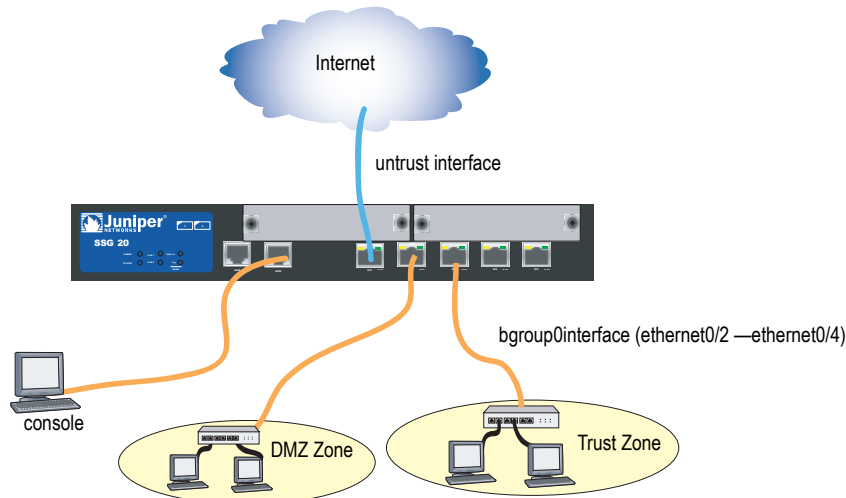
---

## Connect an SSG Device to an Untrusted Network

Figure 5 shows basic network cabling connections for a device. This figure shows two blank PIMs and the 10/100 Ethernet ports are cabled as follows:

- The port labeled 0/0 (ethernet0/0 interface) is connected to the untrust network.
- The port labeled 0/1 (ethernet0/1 interface) is connected to a switch that connects workstations on the DMZ LAN.
- The ports labeled 0/2 through 0/4 (ethernet0/2 through ethernet0/4 interfaces) are connected to a switch that connects workstations to the trusted network.
- The console port is connected to a serial terminal for management access.

**Figure 5: Basic Networking Example**



## Connect Mini PIMs to an Untrusted Network

This section explains how to connect the device mini PIMs to an untrusted network.

### Connecting the ADSL2/2+ Mini PIM

Connect the provided ADSL cable from the ADSL2/2+ mini PIM to your telephone outlet. The ADSL port on the Annex A version of the device uses an RJ-11 connector, while the Annex B version uses an RJ-45 connector. In the case of Annex B models, the cable you connect from the ADSL port to the telephone outlet is identical in appearance and wiring to a straight through 10 Base-T Ethernet cable.

### Connecting Splitters and Microfilters

A *signal splitter* divides the telephone signal into low-frequency voice signals for voice calls and high-frequency data signals for data traffic. Your service provider usually installs the splitter as part of the equipment that connects your site telephone lines to the provider network.

There are also splitters that you may be able to install yourself, depending upon your service-provider equipment. If you are installing such a splitter yourself,



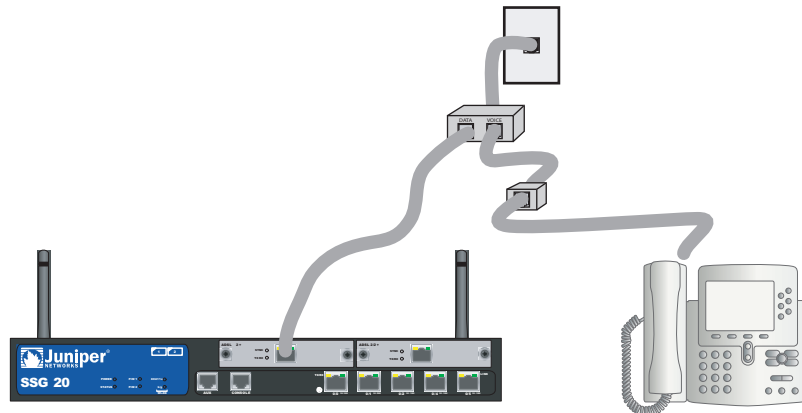
connect the ADSL cable from the device and the telephone line to the appropriate connectors (for example, “data” or “voice”) on the splitter. You connect the other end of the splitter to the telephone outlet.

You may need to install a *microfilter* on each telephone, fax machine, answering machine, or analog modem that connects to the ADSL line. The microfilter filters out high-frequency noise on the telephone line. You install the microfilter on the telephone line between the telephone, fax machine, answering machine, or analog modem and the voice connector on the splitter.

Figure 6 shows an example of a microfilter and a splitter that you install on your site. (You must obtain the appropriate microfilters or splitters from your service provider.)

**Figure 6: Installing a Microfilter and Splitter on Your Network**

New Graphic Needed



### Connecting Other Mini PIMs

To connect the mini PIMs to a device, perform the following steps:

1. Have ready a length of the type of cable used by the interface.
2. Insert the cable connector into the cable-connector port on the interface faceplate.
3. Arrange the cable as follows to prevent it from dislodging or developing stress points:
  - a. Secure the cable so that it is not supporting its own weight as it hangs to the floor.
  - b. Place any excess cable out of the way in a neatly coiled loop.
  - c. Use fasteners to maintain the shape of the cable loops.

To configure the ISDN, E1, T1, or V.92 Mini PIM, see “Mini PIM Configuration” on page 30.

## **Connect the Device to an Internal Network or a Workstation**

You can connect your local area network (LAN) or workstation with the Ethernet and/or wireless interfaces.

### **Connecting Ethernet Ports**

An SSG 20 device contains five Ethernet ports. You can use one or more of these ports to connect to LANs through switches or hubs. You can also connect one or all of the ports directly to workstations, eliminating the need for a hub or switch. You can use either crossover or straight through cables to connect the Ethernet ports to other devices.

### **Connecting the Wireless Antennae**

If you are using the wireless interface, you need to connect the provided antennae on the device. If you have the standard 2dB omnidirectional antennae, use screws to attach them onto the posts marked A and B at the back of the device. Bend each antenna at their elbows, making sure not to put pressure on the bulkhead connectors.



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

## Chapter 3

# Configure the Device

The ScreenOS software is preinstalled on an SSG 20 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 need to perform further configuration for your specific network requirements.

This chapter contains the following sections:

- “Access the Device” on page 18
- “Default Device Settings” on page 21
- “Basic Device Configuration” on page 23
- “Wireless Configuration” on page 27
- “Mini PIM Configuration” on page 30
- “Basic Firewall Protections” on page 37
- “Verify External Connectivity” on page 38
- “Reset the Device to Factory Defaults” on page 38

---

**NOTE:** After you configure a device and verify connectivity through the remote network, you must register your product at [www.juniper.net/support/](http://www.juniper.net/support/) so certain ScreenOS services, such as Deep Inspection Signature Service, 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*.

---

## Access the Device

---

You can configure and manage a device in several ways:

- **Console:** The Console port on the device allows you to 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.
- **WebUI:** The ScreenOS WebUI is a graphical interface available through a Web browser. To initially use the WebUI, the workstation on which you run the Web 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) using secure HTTP (S-HTTP).
- **Telnet/SSH:** Telnet and Secure Shell (SSH) are applications that allows 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, See the *Administration* volume of the *Concepts & Examples Reference Guide* for ScreenOS 5.4.0.
- **NetScreen-Security Manager:** NetScreen-Security Manager is a Juniper Networks enterprise-level management application that enables you to control and manage Juniper Networks firewall/IPSec VPN and SSG devices. For instructions on how to manage your device with NetScreen-Security Manager, refer to the *NetScreen-Security Manager Administrator's Guide*.

### Using a Console Connection

---

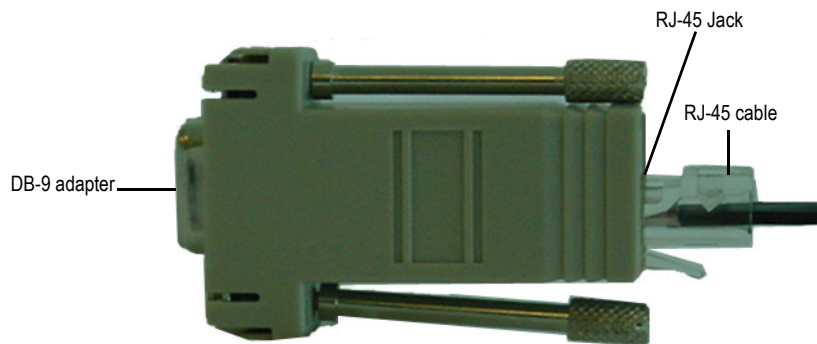
**NOTE:** Use a RJ-45 CAT5 serial cable with a male RJ-45 connector to plug into the Console port on the devices.

---

To establish a console connection, perform the following steps:

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.)

**Figure 7: DB-9 Adapter**



2. Plug the male end of the RJ-45 CAT5 serial cable into the Console port on the SSG 20. (Be sure that the other end of the CAT5 cable is inserted properly and secured in the DB-9 adapter.)
3. Launch a serial terminal-emulation program on your workstation. The required settings to launch a console session with the devices are as follows:
  - Baud rate: 9600
  - Parity: None
  - Data bits: 8
  - Stop bit: 1
  - Flow Control: None
4. If you have not yet changed the default user name and password, enter **netscreen** in 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, see the Concepts and Examples Reference Guide for ScreenOS 5.4.0.

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**.

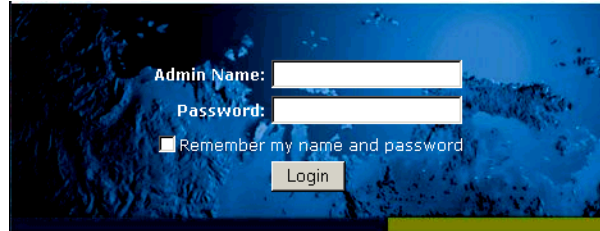
## **Using the WebUI**

To use the WebUI, you must initially be on the same subnetwork as the device. To access the device with the WebUI, perform the following steps:

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 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**.

The WebUI application displays the login prompt as shown in Figure 8.

**Figure 8: WebUI Login Prompt**



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

---

**NOTE:** If you decide to use the Initial Configuration Wizard to configure your device, see “Using the Initial Configuration Wizard” on page I.

---

## Using Telnet

To establish a Telnet connection, perform the following steps:

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 DHCP or is statically configured with an IP address in the 192.168.1.0 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 user name and password, enter **netscreen** in 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 an SSG 20 device.

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

**Table 5: Default Physical Interface to Zone Bindings**

Port Label	Interface	Zone
Console	N/A	N/A
AUX	serial0/0	Null
<b>10/100 Ethernet ports:</b>		
■ 0/0	■ ethernet0/0	Untrust
■ 0/1	■ ethernet0/1	DMZ
■ bgroup0	■ bgroup0 (default IP address is 192.168.1.1/24)	Trust
■ 0/2	■ ethernet0/2	
■ 0/3	■ ethernet0/3	
■ 0/4	■ ethernet0/4	
<b>WAN Mini PIM ports: (x = mini PIM slot, 1 or 2)</b>		
■ ADSL2/2+ (Annex A)	■ adsl(x/0)	Untrust
■ ADSL2/2+ (Annex B)	■ adsl(x/0)	Untrust
■ T1	■ serial(x/0)	Untrust
■ E1	■ serial(x/0)	Untrust
■ ISDN	■ bri(x/0)	Untrust
■ V.92	■ serial(x/0)	Null

A bridge group, bgroup, is designed to allow network users to switch between wired/wireless traffic without having to reconfigure or reboot the device. By default, the ethernet0/2—ethernet0/6 interfaces, labeled as port 0/2—0/6 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.

If you want to set an Ethernet or wireless interface into 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 unset ethernet0/3 from bgroup0 and assign it to the Trust zone with a static IP address of 192.168.3.1/24, do the following:

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

**Table 6: Wireless and Logical Interface Bindings**

SSG 20-WLAN	Interface	Zone
<b>Wireless interface</b>	wireless0/0 (default IP address is 192.168.2.1/24)	Trust
Specifies a wireless interface, which is configurable to operate on 2.4G and/or 5G radio.	wireless0/1-0/3	Null
<b>Logical Interfaces</b>		
Layer2 interface	vlan1 specifies the logical interfaces used for management and VPN traffic termination while the device is in Transparent mode.	N/A
Tunnel interfaces	tunnel.n specifies a logical tunnel interface. This interface is for VPN traffic.	N/A

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 “Wireless Configuration” on page 27.

---

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

---

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

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

---

This section describes optional configuration:

- “Changing the Root Admin Name and Password” on this page
- “Setting the Date and Time” on page 24
- “Administrative Access” on page 25
- “Management Services” on page 25
- “Host and Domain Name” on page 25
- “Default Route” on page 26
- “Management Interface Address” on page 26
- “Backup Untrust Interface Configuration” on page 26

### Changing the Root Admin Name and Password

The root admin user has complete privileges to configure an SSG 20 device. We recommend that you change the default root admin name (`netscreen`) and password (`netscreen`) immediately.

#### WebUI

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

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

---

**NOTE:** Passwords are not displayed in the WebUI.

---

#### CLI

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

## Setting the Date and Time

The time set on an SSG 20 device affects events such as the setup of VPN tunnels. The easiest way to set the date and time on the device is to use the WebUI to synchronize the device system clock with the workstation clock.

### 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 system clock and adjust it according to daylight saving time or click **No** to synchronize the system clock without adjusting for daylight saving time.

You can also use the `set clock` CLI command in a Telnet or Console session to manually enter the date and time for the SSG device.

## Bridge Group Interfaces

By default, the SSG 20 device has Ethernet interfaces ethernet0/2—ethernet0/4 grouped together in the Trust security zone. Grouping interfaces sets interfaces in one subnet. You can unset an interface from a group and assign it to a different security zone. Interfaces must be in the Null security zone before they can be assigned to a group. To place a grouped interface in the Null security zone, use the `unset interface interface port interface` CLI command.

The SSG 20-WLAN devices allow Ethernet and wireless interfaces to be grouped under one subnet.

---

**NOTE:** Only wireless and Ethernet interfaces can be set in a bridge group.

---

To configure a group with Ethernet and wireless interfaces, do the following:

```
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
```

## Administrative Access

By default, anyone in your network can manage a device if they know the login and password. You can configure the device to be managed only from a specific host on your network:

### WebUI

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

IP Address/Netmask: *ip\_addr/mask*

### CLI

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

## Management Services

ScreenOS provides services for configuring and managing the SSG device, such as SNMP, SSL, and SSH, which you can enable on a per-interface basis.

### 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 ethernet0/0 manage web
unset interface ethernet0/0 manage snmp
save
```

## Host 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 the device in the network.

### WebUI

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

Host Name: *name*  
Domain Name: *name*

### CLI

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

## 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 that the device does not have routing information for, the device sends the packet to the destination specified by the default route.

### WebUI

Network > Routing > Routing Entries > New: Enter the following, then click **OK**:

Network Address/Netmask: 0.0.0.0/0.0.0.0  
 Gateway: (select)  
 Interface: serial1/0 (select)  
 Gateway IP Address: *ip\_addr*

### CLI

```
set route 0.0.0.0/0 interface serial1/0 gateway ip_addr
save
```

## Management Interface Address

The Trust interface has the default IP address 192.168.1.1/24 and is configured for management services. If you connect the 0/2—0/4 port on the 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 trust interface. For example, you might want to change the interface to match IP addresses that already exist on your LAN.

## Backup Untrust Interface Configuration

The SSG 20 device allows you to 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 ]** CLI command.
2. Bind the backup interface to the same security zone as the primary interface with the **set interface interface zone zone\_name** CLI 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, do either of the following:

### **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
```

## **Wireless Configuration**

---

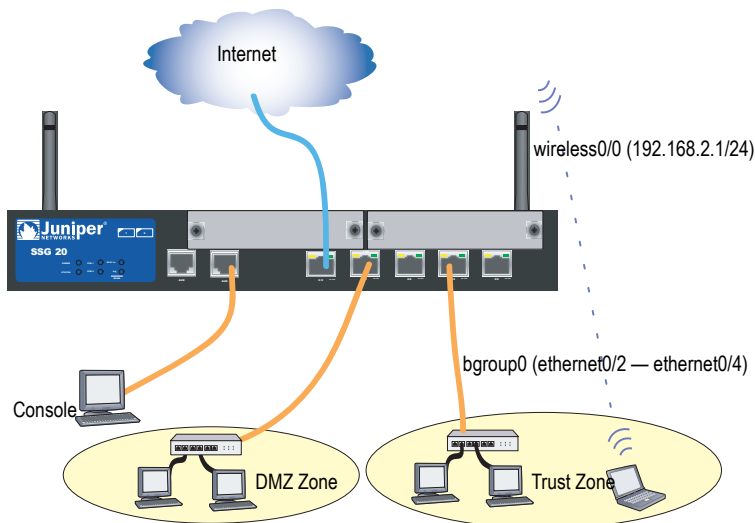
This section provides information for configuring the wireless interface on the SSG 20-WLAN device. To use the wireless local area network (WLAN) capabilities on the device, you must configure at least one Service Set Identifier (SSID) and bind it to a wireless interface.

---

**NOTE:** If you are operating the SSG 20-WLAN device in a country other than the United States or Japan, then you must use the **set wlan country-code** command before a WLAN connection can be established. This command sets the selectable channel range and transmit power level.

---

Figure 9 shows the default configuration for the SSG 20-WLAN device.

**Figure 9: Default SSG 20-WLAN Configuration**

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

By default, the wireless0/1 - wireless0/3 interfaces are defined as Null and do not have IP addresses assigned to them. If you want to use any of the other wireless interfaces, you must configure an IP address for it, assign an SSID to it, and bind it to a security zone.

For more information about WLANs, refer to “Wireless Interface” in the *Concepts and Examples ScreenOS Reference Guide*.

## Wireless Network Configuration

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.

The SSG 20-WLAN device allows you to 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 }** CLI command to set the radio transceivers on the SSG 20-WLAN device.

To set the SSID name **netscreen open**, allow the SSID to be open to all users, bind the SSID to the wireless0/0 interface, and use both radio transceivers, do either of the following:

### WebUI

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

SSID: netscreen open  
Authentication: open  
Encryption: none  
Wireless Interface Binding: wireless0/0 (select)

### CLI

```
set ssid name "netscreen open"  
set ssid "netscreen open" authentication open encryption none  
set ssid "netscreen open" interface wireless0/0  
set interface wireless0/0 wlan both  
set interface wireless0/0 zone trust  
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 up a wireless interface for basic configuration, do the following:

```
set wlan country-code { code_id }  
set interface wireless_interface ip ip_addr/netmask  
set ssid name name_str  
set ssid name_str authentication auth_type encryption encryption_type  
set ssid name_str key-id number  
set ssid name_str interface interface  
set interface wireless_interface wlan both  
save  
exec wlan reactivate
```

To set an ethernet and wireless interface to the same bridge group interface, do the following:

```
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.

---

## Authentication and Encryption

The SSG 20-WLAN supports the following authorization and encryption methods:

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

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 provided “Access the Device” on page 18. Refer to the *Concepts & Examples ScreenOS Reference Guide* for configuration examples, SSID attributes, and CLI commands relating to wireless security configurations.

## Mini PIM Configuration

This section explains how to configure the mini physical interface modules (PIMs):

- “Asymmetrical DSL (ADSL) 2/2 + Interface” on this page
- “The ISDN Interface” on page 34
- “The T1 Interface” on page 35
- “The E1 Interface” on page 36
- “The V.92 Modem Interface” on page 37

### Asymmetrical DSL (ADSL) 2/2+ Interface

Your network uses the ADSL2/2 + interface **adslx/0**, with x representing the mini PIM slot (1 or 2), on the device to connect to the service provider’s network through an Asynchronous Transfer Mode (ATM) virtual circuit. You can configure additional virtual circuits by creating ADSL2/2 + subinterfaces. For more information, see “Virtual Circuits to an ADSL2/2 + Interface” on page 31.

In the WebUI, navigate to the Network > Interfaces > List page to see a list of the current interfaces on the device. If you are using a Telnet or Console session, enter the **get interface** CLI command. You should see that the adslx/0 interface is bound to the Untrust zone.



If you are using the ADSL2/2 + interface to connect to the service provider's network, you must configure the adsl(x/0) interface. To do this, you must obtain the following information from your service provider:

- Virtual Path Identifier and Virtual Channel Identifier (VPI/VCI) values
- ATM Adaptation Layer 5 (AAL5) multiplexing method, which can be one of the following:
  - Virtual Circuit-based multiplexing, in which each protocol is carried over a separate ATM virtual circuit
  - Logical Link Control (LLC) encapsulation, which allows several protocols to be carried on the same ATM virtual circuit (the default multiplexing method)
- Username and password assigned by the service provider for connection to the service provider's network using either Point-to-Point Protocol over Ethernet (PPPoE) or Point-to-Point Protocol over ATM (PPPoA)
- Authentication method, if any, provided for the PPPoE or PPPoA connection
- Optionally, a static IP address and netmask value for your network

### Virtual Circuits to an ADSL2/2+ Interface

To add virtual circuits, you create subinterfaces to the ADSL2/2 + interface. You can create up to 10 ADSL2/2 + subinterfaces. For example, to create a new subinterface named adsl1/0.1 bound to the user-defined zone named **Untrust**:

#### WebUI

Network > Interfaces > New ADSL Sub-IF: Enter the following, click **Apply**:

Interface Name: adsl1/0.1  
VPI/VCI: 8/35  
Zone Name: Untrust (select)

#### CLI

```
set interface adsl 1/0.1 pvc 0 35 zone Untrust  
save
```

You need to configure an ADSL 2/2 + subinterface in the same way as the main ADSL2/2 + interface, including setting the VPI/VCI values, as described in “Connecting the ADSL2/2 + Mini PIM” on page 12. You configure an ADSL2/2 + subinterface independently of the main ADSL2/2 + interface; that is, you can configure a different multiplexing method, VPI/VCI, and PPP client on the subinterface than on the main ADSL2/2 + interface. You can also configure a static IP address on a subinterface, even if the main ADSL2/2 + interface does not have a static IP address. Note that a subinterface and the main ADSL2/2 + interface have to use the same VPI/VCI values if one interface is configured for PPPoA and the other for PPPoE and they both use LLC multiplexing.

## VPI/VCI and Multiplexing Method

Your service provider assigns a VPI/VCI pair for each virtual circuit connection. For example, you may receive the VPI/VCI pair 1/32, which means a VPI value of 1 and a VCI value of 32. These values must match the values that the service provider has configured on the subscriber's side of the Digital Subscriber Line Access Multiplexer (DSLAM).

To configure the VPI/VCI pair 1/32 on the adsl1/0 interface:

### WebUI

Network > Interfaces > Edit (for the adsl1/0 interface): Enter 1/32 in the VPI/VCI field, click **Apply**.

### CLI

```
set interface adsl1/0 pvc 1 32
save
```

By default, the device uses LLC-based multiplexing for each virtual circuit. To configure the VPI/VCI 1/32 on the adslx/0 interface and use LLC encapsulation on the virtual circuit:

### WebUI

Network > Interfaces > Edit (for the adsl1/0 interface): Enter the following, click **Apply**:

```
VPI/VCI: 1 / 32
Multiplexing Method: LLC (selected)
```

### CLI

```
set interface adsl1/0 pvc 1 32 mux llc
save
```

## PPPoE or PPPoA

An SSG 20 device includes both PPPoE and PPPoA clients to connect to the service provider's network over the ADSL link. PPPoE is the most common form of ADSL encapsulation and is intended for termination on each host on your network. PPPoA is used primarily for business class-service as PPP sessions can be terminated on the device. To allow the device to connect to the service provider's network, you need to configure the username and password assigned by the service provider. The configuration for PPPoA is similar to the configuration for PPPoE.

---

**NOTE:** The device supports only one PPPoE session on each virtual circuit.

---

To configure the user name **roswell** and password **area51** for PPPoE and bind the PPPoE configuration to the adsl1/0 interface:

### **WebUI**

Network > PPP > PPPoE Profile > New: Enter the following, click **OK**:

PPPoE Instance: poe1  
Bound to Interface: adsl1/0 (select)  
Username: roswell  
Password: area51

### **CLI**

```
set pppoe name poe1 username roswell password area51
set pppoe name poe1 interface adsl1/0
save
```

There are other PPPoE or PPPoA parameters that you can configure on the device, including method of authentication (by default, the device supports either Challenge Handshake Authentication Protocol or Password Authentication Protocol), idle timeout (default is 30 minutes), and so on. Ask your service provider if there are additional PPPoE or PPPoA parameters that you need to configure to enable proper communications with the service provider's server.

## **Static IP Address and Netmask**

If your ISP gave you a specific, fixed IP address and netmask for your network, then configure the IP address and netmask for the network and the IP address of the router port connected to the device. You need to also specify that the device is to use the static IP address. (Typically, the device acts as a PPPoE or PPPoA client and receives an IP address for the ADSL interface through negotiations with the PPPoE or PPPoA server.)

You need to configure a PPPoE or PPPoA instance and bind it to the adsl1/0 interface, as described in "PPPoE or PPPoA" on page 32. Make sure that you select **Obtain IP using PPPoE** or **Obtain IP using PPPoA** and the name of the PPPoE or PPPoA instance.

To configure the static IP address 1.1.1.1/24 for the network:

### **WebUI**

Network > Interfaces > List > Edit (for the adsl1/0 interface): Enter the following, click **Apply**:

IP Address/Netmask: 1.1.1.1/24  
Static IP: (select)

### **CLI**

```
set interface adsl1/0 ip 1.1.1.1/24
set pppoe name poe1 static-ip
save
```

or

```
set interface adsl1/0 ip 1.1.1.1/24
set pppoa name poa1 static-ip
save
```

To use Domain Name System (DNS) for domain name and address resolution, the computers in your network need to have the IP address of at least one DNS server. If the device receives an IP address for the ADSL2/2+ interface through PPPoE or PPPoA, then it also automatically receives IP addresses for the DNS server(s). If the computers in your network obtain their IP address(es) from the DHCP server on the device, then the computers also obtain these DNS server addresses.

If you assign a static IP address to the ADSL2/2+ interface, then the service provider must give you the IP address(es) of the DNS server(s). You can either configure the DNS server address on each computer in your network or configure the DHCP server on the Trust zone interface so that it provides the DNS server address to each computer.

To configure the DHCP server on the bgroup0 interface to provide the DNS server address 1.1.1.152 to computers in your network:

#### **WebUI**

Network > DHCP > Edit (for the bgroup0 interface) > DHCP Server: Enter 1.1.1.152 for DNS1, click **Apply**.

#### **CLI**

```
set interface bgroup0 dhcp server option dns1 1.1.1.152
save
```

For more information about configuring the ADSL and ADSL2/2+ interfaces, refer to the *Concepts & Examples ScreenOS Reference Guide*.

## **The ISDN Interface**

Integrated Services Digital Network (ISDN) is a set of standards for digital transmission over different media created by the Consultative Committee for International Telegraphy and Telephone (CCITT) and International Telecommunications Union (ITU). As a dial-on-demand service, it has fast call setup and low latency as well as the ability to carry high-quality voice, data, and video transmissions. ISDN is also a circuit-switched service that can be used on both multipoint and point-to-point connections. ISDN provides a service router with a backup connection for network interfaces. The ISDN interface is usually configured as the backup interface of the Ethernet interface to access external networks.

To configure the ISDN interface, do either of the following:

#### **WebUI**

Network > Interfaces > Edit (bri1/0): Enter or select the applicable option value, then click **OK**.

```
BRI Mode: Dial Using BRI
Primary Number: 123456
WAN Encapsulation: PPP
PPP Profile: isdnprofile
```

#### **CLI**

```
set interface bri1/0 dialer-enable
set interface bri1/0 primary-number "123456"
set interface bri1/0 encaps ppp
```

```
set interface bri1/0 ppp profile isdnprofile
save
```

For more information on how to configure the ISDN interface, refer to the *Concepts & Examples ScreenOS Reference Guide*.

To configure the ISDN interface as the backup interface, see “Backup Untrust Interface Configuration” on page 26.

## The T1 Interface

The T1 interface is a basic Physical Layer protocol used by the Digital Signal level 1 (DS-1) multiplexing method in North America. A T1 interface operates at a bit-rate of 1.544 Mbps and can support 24 DS0 channels.

The devices support the following T1 DS-1 standards:

- ANSI T1.107, T1.102
- GR 499-core, GR 253-core
- AT&T Pub 54014
- ITU G.751, G.703

To configure the T1 mini PIM, do either of the following:

### WebUI

Network > Interfaces > Edit (interface) > WAN: Enter or select the applicable option value, click **OK**.

```
WAN Configure: main link
WAN Encapsulation: cisco-hdlc
Zone Name: untrust
IP Address/Netmask 172.18.1.1/24
```

### CLI

```
set interface serial1/0 encap cisco-hdlc
set interface serial1/0 ip 172.18.1.1/24
```

For information on how to configure the T1 interface, refer to the *Concepts & Examples ScreenOS Reference Guide*.

## The E1 Interface

The E1 interface is a standard wide area network (WAN) digital communications format designed to operate over copper facilities at a rate of 2.048 Mbps. Widely used outside North America, E1 is a basic time-division multiplexing scheme used to carry digital circuits.

The devices support the following E1 standards:

- ITU-T G.703
- ITU-T G.751
- ITU-T G.775

To configure the E1 mini PIM, do either of the following:

### WebUI

Network > Interfaces > Edit (interface) > WAN: Enter or select the applicable option value, click **OK**.

WAN Configure: main link  
 WAN Encapsulation: PPP  
 Binding a PPP Profile: junipertest  
 Zone Name: untrust  
 IP Address/Netmask: 172.18.1.1/24

### CLI

```
set interface serial1/0 encapsulation ppp
set ppp profile "junipertest" static-ip
set ppp profile "junipertest" auth type chap
set ppp profile "junipertest" auth local-name "juniper"
set ppp profile "junipertest" auth secret "password"
set interface serial1/0 ppp profile "junipertest"
set interface serial1/0 ip 172.18.1.1/24
set user "server" type wan
set user "server" password "server"
```

For information on how to configure the E1 interface, refer to the *Concepts & Examples ScreenOS Reference Guide*.

## The V.92 Modem Interface

The V.92 interface provides an internal modem to establish a PPP connection to an ISP. You can configure the serial interface as a primary or backup interface, which is used in case of interface failover.

---

**NOTE:** The V.92 interface does not work in transparent mode.

---

To configure the V.92 interface, do either of the following:

### WebUI

Network > Interfaces > Edit (for serial1/0) > Modem: Enter the following, click **OK**:

Modem Name: mod1  
Init String: AT&FS7=255S32=6  
Status: Enable (select)  
Inactivity Timeout: 20

### CLI

```
set interface serial1/0 modem idle-time 20
set interface serial1/0 modem settings mod1 init-strings AT&FS7=255S32=6
set interface serial1/0 modem settings mod1 active
```

For information on how to configure the V.92 modem interface, refer to the *Concepts & Examples ScreenOS Reference 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 and 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 an 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, see the *Attack Detection and Defense Mechanisms* volume in the *Concepts & Examples ScreenOS Reference Guide*.

## Verify 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 enter the following URL: [www.juniper.net](http://www.juniper.net).

## Reset the Device to Factory Defaults

---

If you lose the admin password, you can reset the device to its default settings. This action destroys any existing configurations but restores access to the device.



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

You can restore the device to its default settings in one of the following ways:

- Using a Console connection. For further information, see the Administration chapter in the Administration volume of the *Concepts and Examples ScreenOS Reference Guide*.
- Using the reset pinhole on the back panel of the device, as described in the next section.

### The Reset Pinhole

You can reset the device and restore the factory default settings by pressing the reset pinhole. To perform this operation, you need to either view the device status LEDs on the front panel or start a Console session as described in Using a Console Connection on page 18.

To use the reset pinhole to reset and restore the default settings, perform the following steps:

1. Locate the reset pinhole on the rear panel. Using a thin, firm wire (such as a paper clip), push the pinhole for four to six seconds and then release.

The STATUS LED blinks red. A message on the Console states that erasure of the configuration has started and the system sends an SNMP/SYSLOG alert.



2. Wait for one to two seconds.

After the first reset, the STATUS LED blinks green; the device is now waiting for the second reset. The Console message now states that the device is waiting for a second confirmation.

3. Push the reset pinhole again for four to six seconds.

The Console message verifies the second reset. The STATUS LED glows red for one-half second and then returns to the blinking green state.

The device then resets to its original factory settings. When the device resets, the STATUS LED glows red for one-half second and then glows green. The Console displays device bootup messages. The system generates SNMP and SYSLOG alerts to configured SYSLOG or SNMP trap hosts.

After the device has rebooted, the Console displays the login prompt for the device. The STATUS LED blinks green. The login for username and password is netscreen.

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. If the device did not reset, an SNMP alert is sent to confirm the failure.



## Chapter 4

# Servicing the Device

This chapter describes service and maintenance procedures for an SSG 20 device. It contains the following sections:

- “Tools and Parts Required” on this page
- “Replacing a Physical Interface Module” on page 41
- “Memory Upgrade” on page 44

---

**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. Before working on any equipment, you should be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

---

### Tools and Parts Required

---

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

- Electrostatic bag or antistatic mat
- Electrostatic discharge (ESD) grounding wrist strap
- Phillips screwdriver, 1/8-inch

### Replacing a Physical Interface Module

---

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



**CAUTION:** Make sure the power is off to the device when removing a mini PIM. They are not hot-swappable.

---

## **Removing a Blank Faceplate**

To maintain proper airflow through the SSG 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, do the following:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface 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 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 1/8" slotted screwdriver.
5. Remove the faceplate, then place the faceplate in the electrostatic bag or on the antistatic mat.

## **Removing a Mini PIM**

Mini PIMs are installed in the front panel of the SSG device. A mini PIM weighs less than .2 lb. (106g).

To remove a mini PIM, do the following:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface 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 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:
  - 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. Loosen and remove the screws on each side of the mini PIM faceplate using a 1/8" slotted screwdriver.

8. Grasp the screws on each side of the mini PIM faceplate and slide it out of the device. Place the mini PIM in the electrostatic bag or on the antistatic mat.
9. If you are not reinstalling a mini PIM into the emptied slot, install a blank faceplate over the slot to maintain proper airflow.

**Figure 10: Removing/Installing a Mini PIM**

Graphic needed.

### ***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 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 device. Then slide the mini PIM in until it lodges firmly in the device.



**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" 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 mini PIM status LED glows steadily green to confirm that the mini PIM is online.

## Memory Upgrade

---

You can upgrade an SSG 20 device with a single 128 MB SODIMM DRAM memory module to a 256 MB module.

To upgrade the memory on an SSG 20 device, perform the following steps:

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. Press and release the power button to power off the device. Verify that the POWER LED blinks and then turns off.
3. Use a phillips screwdriver to remove the screws from the top panel of the chassis. The screws are located at the rear and sides of the panel. Keep the screws nearby for use when closing the chassis later.
4. Grip the rear edge of the top panel, lift it up, then remove it.
5. Locate the memory module slot.

**Figure 11: Memory Module Slots**

Graphic needed.

6. Release the 128 MB SODIMM DRAM 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.
7. Grip the long edge of the memory module and slide it out. Set it aside.
8. Insert one of the 256 MB SODIMM DRAM memory modules into the slot from which you just removed the 128 MB SODIMM DRAM 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.

9. To replace the top panel on the chassis, set the front edge of the top panel into the groove that runs along the top front edge of the chassis. Then lower the top panel onto the chassis.
10. Use the phillips screwdriver to tighten the screws you removed earlier, securing the top panel to the chassis.





## Appendix A

# Specifications

This appendix provides general system specifications for an SSG 20 device.

### SSG 20 Physical Specifications

---

**Table 1: SSG 20 Physical Specifications**

Description	Value
Chassis dimensions	294mm X 194.8mm X 44mm (11.5 inches X 7.7 inches X 2 inches)
Device weight	1.53kg (3.3 lbs) without PIMs installed.
ISDN PIM	70g
ADSL Annex A PIM	106g
ADSL Annex B PIM	106g
T1 PIM	75g
E1 PIM	75g
V.92 PIM	79g

### Electrical Specification

---

**Table 2: SSG 20 Electrical Specifications**

Item	Specification
DC input voltage	12 V
DC system current rating	3.34A - 4.16A

## Environmental

---

**Table 3: 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 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)

## Certifications

---

### 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 Power Line Harmonics
- 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

### **European Telecommunications Standards Institute (ETSI)**

- ETSI EN-3000386-2: 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

## **Connectors**

Table 4 lists the RJ-45 connector pinouts for the Console and Modem ports:

**Table 4: Console and Modem Port Connector Pinouts**

<b>RJ-45</b>	<b>Name</b>	<b>I/O</b>	<b>Description</b>	<b>DB-9</b>
1	RTS Out	O	Request to Send	8
2	DTR Out	O	Data Terminal Ready	6
3	TxD	O	Transmit Data	2
4	GND	N/A	Chassis Ground	5
5	GND	N/A	Chassis Ground	5
6	RxD	I	Receive Data	3
7	DSR	I	Data Set Ready	4
8	CTS	I	Clear to Send	7



## Appendix A

# Initial Configuration Wizard

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

### ***Using the Initial Configuration Wizard***

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 II
2. Administrator Login Window on page II
3. WLAN Access Point Window on page II
4. Physical Ethernet Interface Window on page III
5. ADSL2/2 + Interface Window on page IV
6. T1 Interface Windows on page V
7. E1 Interface Windows on page X
8. ISDN Interface Windows on page XII
9. V.92 Modem Interface Window on page XIV
10. Untrust Zone (Ethernet0/0 Interface) Window on page XV
11. DMZ Zone (Ethernet0/1 Interface) Window on page XVI
12. Trust Zone (Ethernet0/2 Interface) Window on page XVI
13. Wireless Interface (wireless0/0) in Trust Zone Window on page XVII
14. Interface Summary Window on page XVIII
15. Physical Ethernet DHCP Interface Window on page XVIII
16. Wireless DHCP Interface Window on page XIX

17. Confirmation Window on page XIX

## 1. Rapid Deployment Window

**Table 1: Rapid Deployment Window**

If your network uses NetScreen-Security Manager, you can use a Rapid Deployment configlet to automatically configure the SSG 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

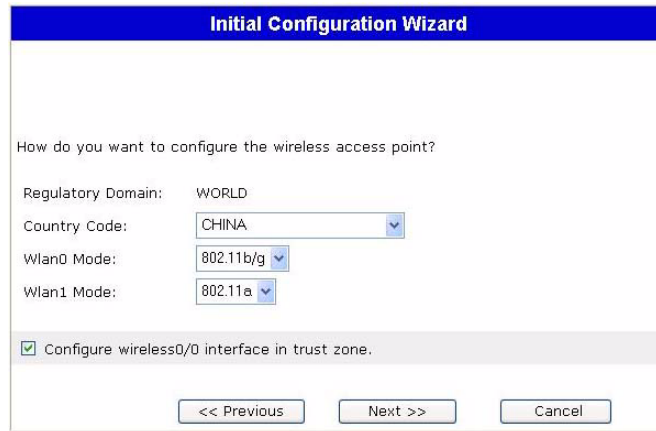
Enter a new administrator login name and password, then Click **Next**.

**Figure 1: Admin Login Window**

## 3. WLAN Access Point Window

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

**Figure 2: Wireless Access Point Country Code Window**

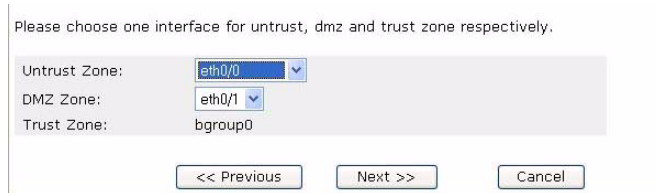


The image shows a screenshot of the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard' in white. Below the title bar, the text 'How do you want to configure the wireless access point?' is displayed. The configuration options are as follows: 'Regulatory Domain:' is set to 'WORLD'; 'Country Code:' is a dropdown menu set to 'CHINA'; 'Wlan0 Mode:' is a dropdown menu set to '802.11b/g'; and 'Wlan1 Mode:' is a dropdown menu set to '802.11a'. Below these options, there is a checked checkbox with the text 'Configure wireless0/0 interface in trust zone.'. At the bottom of the window, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

#### 4. 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. Bgroup0 is prebound to the Trust security zone. Ethernet0/1 is bound to the DMZ security zone but is optional.

**Figure 3:**



The image shows a screenshot of the 'Interface-to-zone bindings' configuration window. The text at the top reads 'Please choose one interface for untrust, dmz and trust zone respectively.'. Below this text, there are three dropdown menus: 'Untrust Zone:' is set to 'eth0/0'; 'DMZ Zone:' is set to 'eth0/1'; and 'Trust Zone:' is set to 'bgroup0'. 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**.

### 5. ADSL2/2+ Interface Window

If you have the ADSL2/2 + mini P1M installed on your device, the following window is displayed. After you have entered the necessary information, click **Next**.

**NOTE:** If you have two ADSL2/2 + mini P1Ms installed on your device and you select the **Multi-link** option, you will see two Physical Layer tabs.

**Figure 4: ADSL2/2+ Interface Configuration Window**

**Table 2:**

Field	Description
<b>Information from Service Provider:</b>	
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.
Operating Mode	Operating mode for the physical line (auto is the default)
IP configuration settings	<ul style="list-style-type: none"> <li>■ Select <b>Dynamic IP via DHCP</b> to enable the device to receive an IP address for ADSL interface from an ISP.</li> <li>■ Select <b>Dynamic IP via PPPoA</b> to enable the device to act as a PPPoA client. Enter the Username and Password assigned by the service provider.</li> <li>■ Select <b>Dynamic IP via PPPoE</b> to enable the device to act as a PPPoE client. Enter the Username and Password assigned by the service provider.</li> <li>■ Select <b>Static IP</b> 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).</li> </ul>

If you do not know what these settings are, please 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 on your device and select the Frame Relay option, the following windows are displayed:

- “T1 Physical Layer Tab Window” on page V
- “T1 Frame Relay Tab Window” on page VII

---

**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.

---

After you have entered the necessary information, click **Next**.

**Figure 5: T1 Physical Layer Tab Window**

The screenshot shows the configuration window for the T1 Physical Layer. At the top, 'WAN Encapsulation' is set to 'Frame Relay' (selected), with 'PPP' and 'Cisco HDLC' as unselected options. Below this, there are two tabs: 'Physical Layer' (active) and 'Frame Relay'. The 'Physical Layer' tab contains the following settings:

- Clocking:**  Internal,  External
- Line Buildout:** 0~132 Feet (dropdown menu)
- Line Encoding:**  Auto Mark Inversion,  8-bits Zero Suppression
- Byte Encoding:**  7-bits per byte,  8-bits per byte
- Frame Checksum:**  16-bits,  32-bits
- Framing Mode:**  Super Frame,  Extended Super Frame
- Idle Cycles Flag:**  0x7E,  0xFF(All Ones)
- Start/End Flags:**  Filler,  Share
- Invert data:**
- Loopback Respond:**
- Time Slots:** 0 (dropdown menu) (0(all active), 1..24(e.g. 2,7-9))

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

**Table 3: Field Description for T1 Physical Layer Tab**

<b>Field</b>	<b>Description</b>
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. <ul style="list-style-type: none"> <li>■ Auto Mark Inversion</li> <li>■ 8-bits zero suppression</li> </ul>
Byte Encoding	Sets the byte encoding on the T1 interface to use 7-bits per byte or 8-bits per byte. Default is 8-bits.
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. <ul style="list-style-type: none"> <li>■ 0x7E (flags)</li> <li>■ 0xFF (ones)</li> </ul>
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 between the T1 interface and the remote channel service unit (CSU).
Time Slots	Sets the use of time slots on a T1 interface. Default is <b>0</b> , all 24 time slots used.

**Figure 6: T1 Frame Relay Tab Window**

**Table 4: Field Description for T1 Frame Relay Tab**

Field	Description
No-Keepalives checkbox	Enables no-keepalives
Type	Sets the frame relay LMI type <ul style="list-style-type: none"> <li>■ ANSI: American National Standards Institute supports data rates up to 8 Mbps downstream and 1 Mbps upstream.</li> <li>■ ITU: International Telecommunications Union supports data rates of 6.144 Mbps downstream and 640 kbps upstream.</li> </ul>
Interface Name	Sets the subinterface name
Inverse ARP	Enables inverse Address Resolution Protocol (ARP) for the subinterface
Frame Relay DLCI	Assigns a DLCI to the subinterface
Interface IP	Sets the IP address for the subinterface
Netmask	Sets the netmask for the subinterface
Gateway	Sets the gateway for the subinterface

If you have the T1 mini PIM installed on your device and select the PPP option, the following windows are displayed:

- “PPP Option with PPP Tab Window” on page VIII
- “PPP Option with Peer User Tab Window” on page VIII

After you have entered the necessary information, click **Next**.

**Figure 7: PPP Option with PPP Tab Window**

WAN Encapsulation:  Frame Relay  PPP  Cisco HDLC

Physical Layer | **PPP** | Peer User

Please create the PPP profile.

PPP Profile Name:

Authentication:  Any  CHAP  PAP  None

Local User:

Password:

Static IP:

Please configure the serial1/0 interface.

Interface IP:

Netmask:

Gateway:

**Table 5: Field Description for PPP Option with PPP Tab**

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 8: PPP Option with Peer User Tab Window**

WAN Encapsulation:  Frame Relay  PPP  Cisco HDLC

Physical Layer | PPP | **Peer User**

Peer User:

Password:

Status:  Enable  Disable

**Table 6: Field Description for PPP Option with Peer User Tab**

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 on your device and select the Cisco HDLC option, the following window is displayed.

**Figure 9: Cisco HDLC Option with Cisco HDLC Tab Window**

WAN Encapsulation:  Frame Relay  PPP  Cisco HDLC

Physical Layer Cisco HDLC

Interface IP:

Netmask:

Gateway:

**Table 7: Field Description for Cisco HDLC Option**

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 for the T1 Cisco HDLC interface

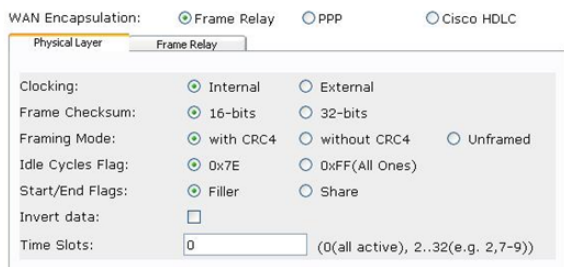
### 7. E1 Interface Windows

If you have the E1 mini PIM installed on your device and select the Frame Relay option, the following windows are displayed:

- “E1 Physical Layer Tab Window” on page X
- “E1 Frame Relay Tab Window” on page XI

**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 10: E1 Physical Layer Tab Window**



**Table 8: Field Description for E1 Physical Layer Tab**

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 <ul style="list-style-type: none"> <li>■ 0x7E (flags)</li> <li>■ 0xFF (ones)</li> </ul>
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 T1 interface. Default is 0, all 32 time slots used

**Figure 11: E1 Frame Relay Tab Window**

WAN Encapsulation:  Frame Relay  PPP  Cisco HDLC

Physical Layer **Frame Relay**

No-Keepalive:

Type:  ANSI  ITU

Please configure the sub interface.

Interface Name: serial2/0. 1

Inverse ARP:

Frame Relay DLCI:  (16~1022)

Interface IP:

Netmask:

Gateway:

**Table 9: Field Descriptions for the Frame Relay Tab**

Field	Description
No-Keepalives checkbox	Enables no-keepalives
Type	Sets the frame relay LMI type <ul style="list-style-type: none"> <li>■ ANSI: American National Standards Institute supports data rates up to 8 Mbps downstream and 1 Mbps upstream.</li> <li>■ ITU: International Telecommunications Union supports data rates of 6.144 Mbps downstream and 640 kbps upstream.</li> </ul>
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
Interface IP	Sets the IP address for the subinterface
Netmask	Sets the netmask for the subinterface
Gateway	Sets the gateway for the subinterface

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

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

## 8. ISDN Interface Windows

If you have the ISDN mini PIM installed on your device, a physical layer tab window similar to the following is displayed.

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

**Figure 12: ISDN Physical Layer Tab Window**

**Table 10: Field Description for ISDN Physical Layer Tab**

Field	Description
Switch Type	Sets the service provider switch type: <ul style="list-style-type: none"> <li>■ att5e - At&amp;T 5ESS</li> <li>■ ntdms100 - Nortel DMS 100</li> <li>■ ins-net - NTT INS-Net</li> <li>■ etsi - European variants</li> <li>■ ni1 - National ISDN-1</li> </ul>
SPID1	Service Provider ID, usually a seven-digit telephone number with some optional numbers. Only the DMS-100 and NI 1 switch types require SPIDs. The DMS-100 switch type has two SPIDs assigned, one for each B-channel.
SPID2	Back up 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	The ISDN network billing number. TR6 switch type cannot use this field.
T310 Value	The timeout value (in seconds) before sending a DISC to the network. Default value is 10.
Sending Complete checkbox	Enables sending complete information to outgoing setup message. Usually only used in Hong Kong and Taiwan.

If you have the ISDN mini PIM installed on your device, you will see the Leased Line Mode and Dial Using BRI checkboxes. Selecting **either** or **none** displays a window similar to the following.



**Figure 13: ISDN Licensed-Line, Leased-Line, and Dial Using BRI Tabs Window**

Leased Line Mode (128Kbps):

Dial Using BRI:

Physical Layer **Leased-Line**

Please create the PPP profile.

PPP Profile Name:

Authentication:  Any  CHAP  PAP  None

Local User:

Password:

Static IP:

Interface IP:

Netmask:

Gateway:

**Table 11: Field Descriptions for the ISDN Licensed-Line, Leased-Line, and Dial Using BRI Tabs**

Field	Description
PPP Profile Name	Sets a PPP profile name to the ISDN interface
Authentication	Sets the PPP authentication type: <ul style="list-style-type: none"> <li>■ Any</li> <li>■ CHAP: Challenge Handshake Authentication Protocol</li> <li>■ PAP: Password Authentication Protocol</li> <li>■ None</li> </ul>
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
Netmask	Sets the netmask
Gateway	Sets the gateway address

## 9. V.92 Modem Interface Window

If you have the V.92 mini PIM installed on your device, the following window is displayed:

**Figure 14: V.92 Modem Interface Window**

Modem Name:	<input type="text" value="modem"/>
Init Strings:	<input "="" type="text" value="AT&amp;F1E1Q0V1S7="/>
ISP Name:	<input type="text" value="isp"/>
Primary Number:	<input type="text"/>
Alternative Number:	<input type="text"/> (Optional)
Login Name:	<input type="text"/>
Password:	<input type="text"/>

**Table 12: Field Descriptions for V.92 Modem**

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

## 10. Untrust Zone (Ethernet0/0 Interface) Window

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

**Figure 15: ethernet0/0 Interface Window**

The screenshot shows a configuration window for the ethernet0/0 interface. It features three radio button options for IP assignment: 'Dynamic IP via DHCP', 'Dynamic IP via PPPoE', and 'Static IP'. The 'Static IP' option is currently selected. Under 'Dynamic IP via PPPoE', there are input fields for 'Username:' and 'Password:'. Under 'Static IP', there are input fields for 'Interface IP:', 'Netmask:', and 'Gateway:'.

**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.

### 11. DMZ Zone (Ethernet0/1 Interface) Window

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

**Figure 16: Ethernet0/1 Interface Window**



**Table 14: Field Descriptions for the Ethernet0/1 Interface**

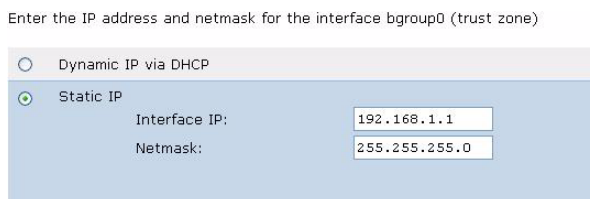
Field	Description
Dynamic IP via DHCP	Enables the device to receive an IP address for the DMZ zone interface from an ISP.
Static IP	Assigns a unique and fixed IP address to the DMZ zone interface. Enter the DMZ zone interface IP and netmask.

### 12. Trust Zone (Ethernet0/2 Interface) Window

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

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

**Figure 17: Trust Zone (Ethernet0/2 Interface) Window**



**Table 15: Field Descriptions for the Trust Zone Interface**

Field	Description
Dynamic IP via DHCP	Enables the device to receive an IP address for the Trust zone interface from an ISP.
Static IP	Assigns a unique and fixed IP address to the Trust zone interface. Enter the Trust Zone Interface IP and Netmask.

### 13. Wireless Interface (wireless0/0) in Trust Zone Window

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), see the *Concepts and Examples ScreenOS Reference Guide*.

**Figure 18: Wireless0/0 Interface Window**

**Table 16: Field Descriptions for Wireless0/0 Interface**

Field	Description
Wlan Mode	Sets the WLAN radio mode: <ul style="list-style-type: none"> <li>■ 802.11 a</li> <li>■ 802.11 b/g</li> <li>■ 802.11 a/b/g</li> </ul>
SSID	Sets the SSID name.
Authentication and Encryption	Sets the WLAN interface authentication and encryption. <ul style="list-style-type: none"> <li>■ <b>Open</b> authentication, the default, allows anyone to access the device. There is no encryption for this authentication option.</li> <li>■ <b>WPA Pre-Shared Key</b> authentication sets the Pre-Shared Key (PSK) or passphrase that must be entered when accessing wireless connectivity. 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) encryption type for this option, or select <b>Auto</b> to allow either option.</li> </ul>
Interface IP	Sets the WLAN interface IP address.
Netmask	Sets the WLAN interface netmask.

After you have configured the WAN interfaces with, you will see the Interface Summary Window. Check your interface configuration, then click **Next** when ready to proceed. The Physical Ethernet DHCP Interface Window appears.

## 14. Interface Summary Window

Before proceeding further, review the following interface settings.

eth0/0 Configuration:			
Interface eth0/0:	dhcp		
eth0/1 Configuration:			
Interface eth0/1:	dhcp		
bgroup0 Configuration:			
Interface bgroup0:	static		
Interface IP:	192.168.1.1	Netmask:	255.255.255.0

```

set interface eth0/0 zone untrust
set interface eth0/0 dhcp-client enable
set interface eth0/1 zone dmz
set interface eth0/1 dhcp-client enable
set interface bgroup0 zone trust
set interface bgroup0 ip 192.168.1.1 255.255.255.0
    
```

Click Next to enter other configuration

<< Previous    Next >>    Cancel

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.

## 15. Physical Ethernet DHCP Interface Window

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.

Yes

IP Address Range Start:

End:

DNS Server 1 (optional):

DNS Server 2 (optional):

No

<< Previous    Next >>    Cancel

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.

## 16. Wireless DHCP Interface Window

Do you want the Juniper device to dynamically assign IP addresses to your local **wireless** hosts using DHCP? If so, select Yes and enter an IP address range from which to assign the addresses.

Yes

IP Address Range Start

End

DNS Server 1 (optional)

DNS Server 2 (optional)

No

<< Previous    Next >>    Cancel

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

## 17. Confirmation Window

Before proceeding further, review the following all device settings.

Admin Login:	netscreen	Password:	*****
<b>eth0/0 Configuration:</b>			
Interface eth0/0:	dhcp		
<b>eth0/1 Configuration:</b>			
Interface eth0/1:	dhcp		
<b>bgroup0 Configuration:</b>			
Interface bgroup0:	static		
Interface IP:	192.168.1.1	Netmask:	255.255.255.0

```
set admin password "netscreen"
set interface eth0/0 zone untrust
set interface eth0/0 dhcp-client enable
set interface eth0/1 zone dmz
set interface eth0/1 dhcp-client enable
set interface bgroup0 zone trust
```

Click Next to save CLI into device.

<< Previous    Next >>    Cancel





# Index

## A

AAL5 multiplexing 31

adding virtual circuit 31

## ADSL

    configuring interface 30

    connecting the cable 13

    connecting the port 13

Annex A 13

Annex B 13

antennae 16

ATM Adaptation Layer 5 31

## B

backup interface to Untrust zone 26

## C

configuration

    management services 25

## M

management services 25

multiplexing, configuring 32

## P

Point-to-Point Protocol over ATM

*See* PPPoA

Point-to-Point Protocol over Ethernet

*See* PPPoE

PPPoA 31

PPPoE 31

## R

reset pinhole, using 38

## S

static IP address 31

## U

Untrust zone, configuring backup interface 26

## V

virtual circuit, adding 31

Virtual Path Identifier/Virtual Channel Identifier

*See* VPI/VCI

VPI/VCI 31

    configuring 32

## W

## Wireless

    antennae 16

    using the default interface 16

