



**Security Products**

# **SSG 5 Hardware Installation and Configuration Guide**

**Juniper Networks, Inc.**

1194 North Mathilda Avenue  
Sunnyvale, CA 94089

USA

408-745-2000

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

## Copyright Notice

Copyright © 2009 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

## FCC Statement

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

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

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

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

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

## Disclaimer

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

# Table of Contents

	About This Guide .....	5
	Organization .....	6
	Conventions .....	6
	Web User Interface Conventions .....	6
	Command Line Interface Conventions .....	7
	Requesting Technical Support .....	7
	Self-Help Online Tools and Resources .....	8
	Opening a Case with JTAC .....	8
	Feedback .....	8
Chapter 1	Hardware Overview .....	9
	Front Panel .....	9
	Port Descriptions .....	9
	Device Status LEDs .....	10
	Ethernet Port LEDs .....	12
	Back Panel .....	12
	Power Connector .....	13
	Radio Transceivers .....	13
	Grounding Lug .....	13
	Antennae Types .....	13
	USB Port .....	14
Chapter 2	Installing and Connecting the Device .....	15
	Before You Begin .....	16
	Installing Equipment .....	16
	Rack Mounting .....	16
	Desk Mounting .....	17
	Organizing Interface Cables .....	18
	Connecting Power .....	18
	Connecting the Device to a Network .....	18
Chapter 3	Configuring the Device .....	21
	Accessing the Device .....	22
	Using a Console Connection .....	22
	Using the WebUI .....	24
	Using Telnet .....	24
	Default Device Settings .....	25
	Basic Device Configuration .....	26
	Admin Name and Password .....	27
	Administrative Access .....	27
	Interface IP Address .....	27
	Management Services .....	28

	Hostname and Domain Name .....	28
	Date and Time.....	28
	Default Route.....	29
	Bridge Group Interfaces .....	29
	Backup Untrust Interface Configuration .....	30
	Basic Wireless Configuration.....	31
	WAN Configuration .....	35
	ISDN Interface .....	35
	V.92 Modem Interface .....	36
	Basic Firewall Protections .....	37
	Verifying External Connectivity.....	37
	Restarting the Device .....	38
	Restarting the Device with the CLI Reset Command .....	38
	Restarting the Device with the WebUI .....	38
	Resetting the Device to Factory Defaults .....	39
	Device Serial Number .....	39
	unset all .....	40
	Reset Pinhole Button .....	40
Chapter 4	Servicing the Device .....	43
	Required Tools and Parts .....	43
	Upgrading Memory .....	43
Appendix A	Specifications .....	47
	Physical.....	47
	Electrical .....	47
	Environmental Tolerance .....	48
	Certifications.....	48
	RoHS and WEEE .....	49
	Connectors.....	49
Appendix B	Initial Configuration Wizard .....	51
Appendix C	Country Code and Channel Information .....	65
	Index.....	67

# About This Guide

The Juniper Networks Secure Services Gateway (SSG) 5 device is an integrated router and firewall platform. It provides Internet Protocol Security (IPSec) virtual private network (VPN) and firewall services for a branch office or a retail outlet.

Juniper Networks offers six models of the SSG 5 device:

- SSG 5 Serial
- SSG 5 Serial-WLAN
- SSG 5 V.92
- SSG 5 V.92-WLAN
- SSG 5 ISDN
- SSG 5 ISDN-WLAN

The WLAN models support wireless local area networks (WLANs).

---

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

---

## Organization

---

This guide contains the following sections:

- Chapter 1, “Hardware Overview,” describes the chassis and components for the SSG 5 device.
- Chapter 2, “Installing and Connecting the Device,” describes how to mount the SSG 5 device and how to connect it to your network.
- Chapter 3, “Configuring the Device,” describes how to configure and manage the SSG 5 device and how to perform some basic configuration tasks.
- Chapter 4, “Servicing the Device,” describes service and maintenance procedures for the SSG 5 device.
- Appendix A, “Specifications,” provides general system specifications for the SSG 5 device.
- Appendix B, “Initial Configuration Wizard,” provides detailed information about using the Initial Configuration Wizard (ICW) for the SSG 5 device.
- Appendix C, “Country Code and Channel Information,” provides information regarding wireless network deployment.

## Conventions

---

This guide uses the conventions described in the following sections:

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

### **Web User Interface Conventions**

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

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

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

Address Name: addr\_1  
IP Address/Domain Name:  
IP/Netmask: (select), 10.2.2.5/32  
Zone: Untrust

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

The navigation tree also provides a Help > Config Guide configuration page to help you configure security policies and Internet Protocol Security (IPSec). Select an option from the list and follow the instructions on the page. Click the ? character in the upper left for Online Help on the Config Guide.

## Command Line Interface Conventions

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

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

In examples:

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

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

---

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

---

## Requesting Technical Support

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

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

## Self-Help Online Tools and Resources

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

- Find CSC offerings—<http://www.juniper.net/customers/support/>
- Find product documentation—<http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base—<http://kb.juniper.net/>
- Download the latest versions of software and review your release notes—<http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications—<http://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum—<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Manager—<http://www.juniper.net/customers/cm/>
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool—<https://tools.juniper.net/SerialNumberEntitlementSearch/>

## Opening a Case with JTAC

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

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

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

## Feedback

---

If you find any errors or omissions in this document, contact Juniper Networks at [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net).



## Chapter 1

# Hardware Overview

This chapter provides detailed descriptions of the SSG 5 chassis and its components. It contains the following sections:

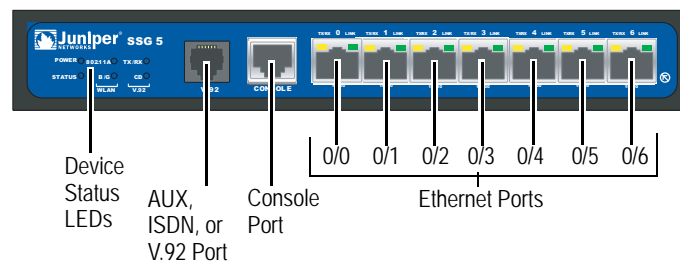
- “Front Panel” on page 9
- “Back Panel” on page 12

### Front Panel

---

Figure 1 shows the front panel of an SSG 5 device.

**Figure 1: SSG 5 Front Panel**



The following sections describes the elements on the front panel of an SSG 5 device:

- “Port Descriptions” on page 9
- “Device Status LEDs” on page 10
- “Ethernet Port LEDs” on page 12

### *Port Descriptions*

Table 1 describes the function, connector type, and speed/protocol of the ports on the front panel of the SSG 5 device.

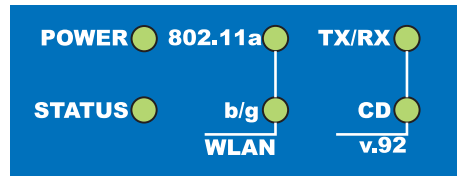
**Table 1: SSG 5 Ports**

Item	Description	Connector	Speed/Protocol
Ethernet 0/0 to 0/6 Ports	<p>Enables ethernet connections to workstations or a LAN connection through a switch or hub. These connections also allow you to manage the device through a Telnet session or the WebUI.</p> <p>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 <b>ethernet0/0</b> through <b>ethernet0/6</b>. For the default zone bindings for each Ethernet port, see “Default Device Settings” on page 27.</p>	RJ-45	10/100 Mbps Ethernet Autosensing duplex and auto MDI/MDIX
USB Port	Enables a 1.1 USB connection with the device.	-	12M (full speed) or 1.5M (low speed)
Console Port	<p>The console port is an RJ-45 serial data terminal equipment (DTE) port that can be used for either local or remote administration. For local administration, connect the port to a terminal with an RJ-45-to-DB-9 (female-to-male) straight-through serial cable. For remote administration, connect the port to a workstation with an RJ-45-to-DB-9 (female-to-male) serial cable with a null modem adapter.</p> <p>See “Connectors” on page 49 for the RJ-45 connector pinouts.</p>	RJ-45	9600 bps/RS-232C serial
AUX Port	<p>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.</p> <p>See “Connectors” on page 49 for the RJ-45 connector pinouts.</p>	RJ-45	9600 bps — 115 Kbps/RS-232C serial
V.92 Modem	Enables a primary or backup Internet or untrusted network connection to a service provider.	RJ-11	9600 bps — 115 Kbps/RS-232 serial autosensing duplex and polarity
ISDN Port	Enables the ISDN line to be used as the untrust or backup interface. (S/T)	RJ-45	B-channels at 64 Kbps Leased line at 128 Kbps

### Device Status LEDs

The Device status LEDs display information about critical device functions. Figure 2 shows the position of each status LED on the front of the SSG 5 V.92-WLAN device. The device LEDs differ depending on the version of the SSG 5 device.

Figure 2: Device Status LEDs (SSG 5 V.92-WLAN Shown, Others Similar)



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

Table 2: Device Status LED Descriptions

Type	Name	Color	State	Description
All SSG 5 Devices	POWER	Green	On steadily	Indicates that the device is receiving power.
			Off	Indicates that the device is not receiving power.
		Red	On steadily	Indicates that the device is not operating normally.
			Off	Indicates that the device is operating normally.
	STATUS	Green	On steadily	Indicates that the device is starting or performing diagnostics.
			Blinking	Indicates that the device is operating normally.
		Red	Blinking	Indicates that there was an error detected.
SSG 5 ISDN	CH B1	Green	On steadily	Indicates that B-Channel 1 is active.
SSG 5 ISDN-WLAN			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.
SSG 5 V.92	TX/RX	Green	Blinking	Indicates that traffic is passing through.
SSG 5 V.92-WLAN			Off	Indicates that no traffic is passing through.
	CD	Green	On steadily	Indicates that the link is active.
			Off	Indicates that the serial interface is not in service.
SSG 5 Serial-WLAN	802.11A	Green	On steadily	Indicates that a wireless connection is established but there is no link activity.
SSG 5 V.92-WLAN			Blinking	Indicates that a wireless connection is established. The data rate is proportional to the blink activity.
SSG 5 ISDN-WLAN			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	Indicates that a wireless connection is established. The data rate is proportional to the blink activity.
			Off	Indicates that there is no wireless connection established.

## Ethernet Port LEDs

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

**Figure 3: Ethernet Port LEDs**

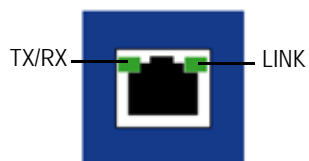


Table 3 describes the Ethernet port LEDs.

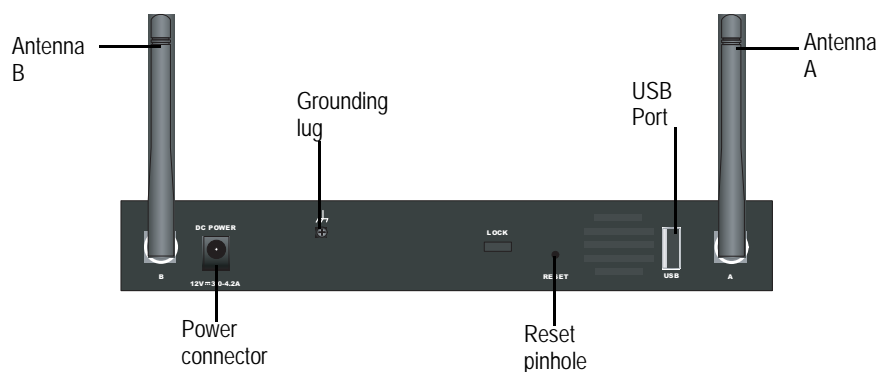
**Table 3: Ethernet Port LEDs**

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

## Back Panel

Figure 4 shows the back panel of the SSG 5 device.

**Figure 4: Back Panel of an SSG 5 Device**



The following sections describe the elements on the back panel of the SSG 5 device:

- “Power Connector” on page 13
- “Radio Transceivers” on page 13
- “Grounding Lug” on page 13
- “Antennae Types” on page 13
- “USB Port” on page 14

---

**NOTE:** Only SSG 5-WLAN devices have the antennae connectors.

---

## Power Connector

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

---

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

---

## Radio Transceivers

The SSG 5 wireless transceivers enable a direct connection to workstations in the vicinity of a wireless radio connection. Table 4 shows information for the transceivers.

**Table 4: Radio Transceiver Information**

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

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

## Grounding Lug

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

To ground the device before connecting power, 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 5-WLAN devices support three types of custom-built radio antennae:

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

- **External directional antenna** — The external directional antenna provides 2dBi unidirectional coverage and is appropriate for locations like hallways and outer walls (with the antenna facing inward).

## USB Port

The USB port on the back panel of an SSG 5 device accepts a universal serial bus (USB) storage device.

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

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

To transfer data between the USB storage device and an SSG 20:

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



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

---

4. Remove the USB storage device.

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

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

## Chapter 2

# Installing and Connecting the Device

This chapter describes how to mount an SSG 5 device and connect cables and power to the device. This chapter contains the following sections:

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

---

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

---

## Before You Begin

---

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



**CAUTION:** To prevent abuse and intrusion by unauthorized personnel, install the SSG 5 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.

## Installing Equipment

---

The following sections describe how to rack-mount or desk-mount the SSG 5 device:

- “Rack Mounting” on page 16
- “Desk Mounting” on page 17

The mounting kits may be purchased separately.

To rack-mount the SSG 5 device, you must have a Number-2 phillips screwdriver (not provided) and screws that are compatible with the equipment rack (included in the kit).

---

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

---

### ***Rack Mounting***

To rack-mount an SSG 5 device:

1. Unscrew the mounting brackets on the tray with a phillips screwdriver.

---

**NOTE:** To install an SSG 5-WLAN with the optional antennae, you must remove the existing antennae and then connect the new antenna through the side hole.

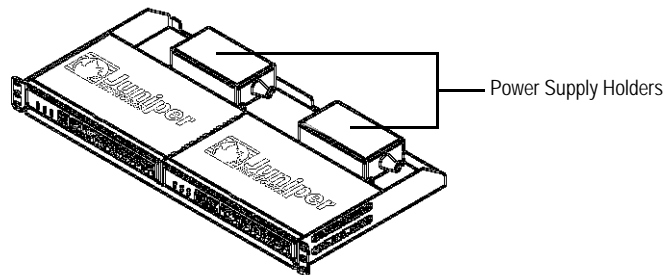
---

2. Align the bottom of the device with the base holes on the tray.



3. Pull the device forward to lock it in the base holes on the tray.
4. Using the screws, attach the mounting brackets to the device and the tray.
5. Place the power supply in the supply holder, then plug the power adapter into the device.
6. To install a second SSG 5 device, repeat steps 1 through 5, then continue.

**Figure 5: SSG 5 Rack Mounting**



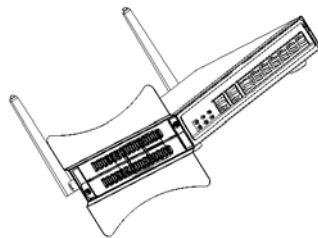
7. Mount the tray on the rack with the screws provided.
8. Plug in the power supply to the power outlet.

## Desk Mounting

To desk-mount an SSG 5 device:

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

**Figure 6: SSG 5 Desk Mounting**



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

## Organizing Interface Cables

---

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

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

## Connecting Power

---

To connect the power to a device:

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



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

---

## Connecting the Device to a Network

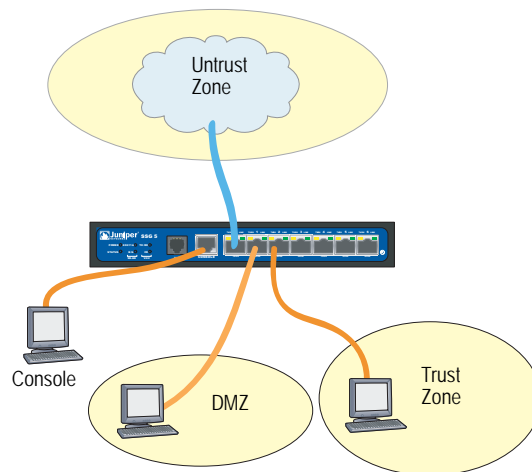
---

This section provides basic information on how to physically connect the SSG 5 device to a network.

To connect the necessary cables as shown in Figure 7:

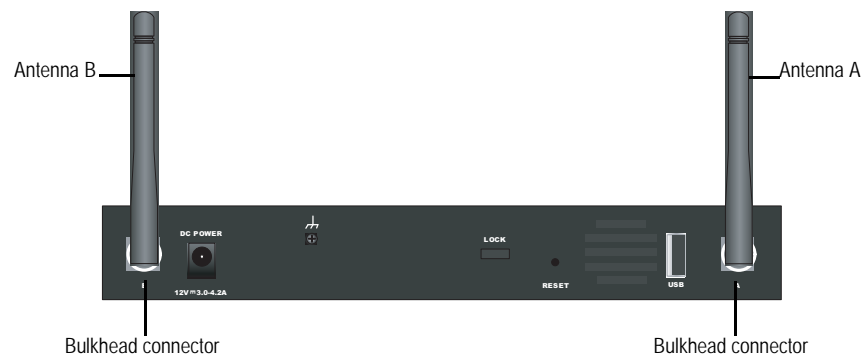
1. Connect an RJ-45 cable from the port labeled **0/0** (ethernet0/0 interface) to the external switch or router. The ethernet0/0 interface is prebound to the Untrust security zone.
2. Connect an RJ-45 cable from the port labeled **0/1** (ethernet0/1 interface) to a switch or router in the DMZ security zone.
3. Connect an RJ-45 cable from the port labeled **0/2** (bgroup0 interface) to a switch or router in the Trust security zone.
4. Connect an RJ-45 cable from the Console port using the instructions provided in “Using a Console Connection” on page 22 for management access.

Figure 7: Basic Cabling Example



5. If you want to connect to your device through wireless, you must first connect the provided antennae to the device. If you have the standard 2dB diversity antennae, use screws to attach them onto the RPSMA posts marked A and B at the back of the device. Bend each antenna at its elbows, making sure not to put pressure on the bulkhead connectors (see Figure 8).

Figure 8: SSG 5-WLAN Antennae Location



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



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



## Chapter 3

# Configuring the Device

ScreenOS software is preinstalled on SSG 5 devices. When the device is powered on, it is ready to be configured. While the device has a default factory configuration that lets you initially connect to the device, you need to perform further configuration for your specific network requirements.

This chapter contains the following sections:

- “Accessing the Device” on page 22
- “Default Device Settings” on page 25
- “Basic Device Configuration” on page 26
- “Basic Wireless Configuration” on page 31
- “WAN Configuration” on page 35
- “Basic Firewall Protections” on page 37
- “Verifying External Connectivity” on page 37
- “Restarting the Device” on page 38
- “Resetting the Device to Factory Defaults” on page 39

---

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

---

## Accessing the Device

---

You can configure and manage the SSG 5 device in several ways:

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

### Using a Console Connection

---

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

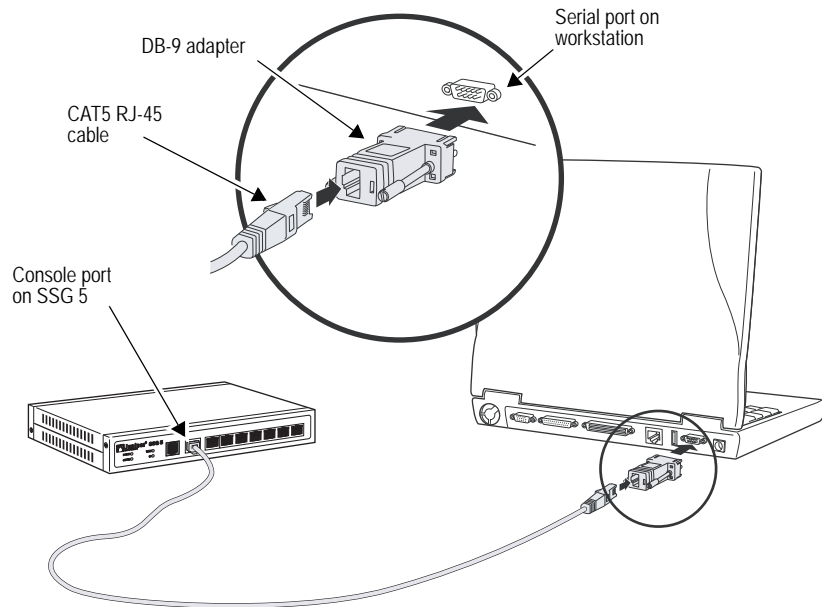
---

To establish a console connection with the device:

1. Plug the female end of an RJ-45-to-DB-9 adapter into the serial port of your workstation, making sure it is properly secured. (RJ-45-to-DB-9 adapters can be purchased from Juniper Networks. See “Connectors” on page 49 for pin numbering information.)
2. Plug one end of the RJ-45 CAT5 cable into the DB-9 adapter.

3. Plug the other end of the RJ-45 CAT5 cable into the Console port on the SSG 5 device. Figure 9 shows the arrangement of the cable and adapter.

**Figure 9: Establishing a Console Connection**



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

For information on how to configure the device with the CLI commands, refer to the *Concepts & Examples ScreenOS Reference Guide*.

6. (Optional) By default, the console times out and terminates automatically after 10 minutes of idle time. To remove the timeout, enter **set console timeout 0**.

## Using the WebUI

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

1. Connect your workstation to the 0/2 — 0/6 port (bgroup0 interface in the Trust zone) on the device.
2. Ensure that your workstation is configured for DHCP or is configured with a static IP address in the 192.168.1.0/24 subnet.
3. Launch your browser, enter the IP address for the bgroup0 interface (the default IP address is 192.168.1.1/24), then press **Enter**.

---

**NOTE:** When the device is accessed through the WebUI the first time, the Initial Configuration Wizard (ICW) appears. If you decide to use the ICW to configure your device, see “Initial Configuration Wizard” on page 51.

---

The WebUI application displays the login prompt.

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

## Using Telnet

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

1. Connect your workstation to any Ethernet port from 0/2 to 0/6 (bgroup0 interface in the Trust zone) on the device.
2. Ensure that your workstation is configured for DHCP or is configured with a static IP address in the 192.168.1.0/24 subnet.
3. Start a Telnet client application to the IP address for the bgroup0 interface (the default IP address is 192.168.1.1). For example, enter **telnet 192.168.1.1**.

The Telnet application displays the login prompt.

4. If you have not yet changed the default login for the login name and password, enter **netscreen** at both the login and password prompts. (Use lowercase letters only. The login and password fields are both case-sensitive)
5. (Optional) By default, the console times out and terminates automatically after 10 minutes of idle time. To remove the timeout, enter **set console timeout 0**.



## Default Device Settings

This section describes the default settings and operation of the SSG 5 device.

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

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

Port Label	Interface	Zone
<b>10/100 Ethernet ports:</b>		
0/0	ethernet0/0	Untrust
0/1	ethernet0/1	DMZ
0/2	bgroup0 (ethernet0/2)	Trust
0/3	bgroup0 (ethernet0/3)	Trust
0/4	bgroup0 (ethernet0/4)	Trust
0/5	bgroup0 (ethernet0/5)	Trust
0/6	bgroup0 (ethernet0/6)	Trust
AUX	serial0/0	Null
<b>WAN ports:</b>		
ISDN	bri0/0	Untrust
V.92	serial0/0	Null

Bridge groups (bgroups) let network users switch between wired and wireless traffic without having to reconfigure or reboot their workstations. By default, the ethernet0/2 — ethernet0/6 interfaces, labeled as ports 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.

You can change the default IP address on the bgroup0 interface to match the addresses on your LAN and WLAN. For configuring a wireless interface to a bgroup, see “Basic Wireless Configuration” on page 31.

---

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

---

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

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

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

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

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

## Basic Device Configuration

The following sections describe the basic configuration tasks required to place the SSG 5 device in operation:

- “Admin Name and Password” on page 27
- “Administrative Access” on page 27
- “Interface IP Address” on page 27
- “Management Services” on page 28
- “Hostname and Domain Name” on page 28
- “Date and Time” on page 28
- “Default Route” on page 29
- “Bridge Group Interfaces” on page 29
- “Backup Untrust Interface Configuration” on page 30

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

## Admin Name and Password

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

To change the admin name and password:

### WebUI

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

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

### CLI

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

## Administrative Access

By default, anyone in your network can manage the device if they know the admin name and password.

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

### WebUI

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

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

### CLI

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

## Interface IP Address

The bgroup0 interface has the default IP address 192.168.1.1/24 and is preconfigured for management services. You can configure the device using a management service such as Telnet by connecting a workstation to any of the bgroup0 ports on the device. The workstation must have an IP address in the 192.168.1.1/24 subnet.

To change the default interface IP address on the device:

### WebUI

Network > Interfaces > Edit (for bgroup0): Enter the following, then click **OK**:

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

**CLI**

```
set interface bgroup0 ip ip_addr/mask
save
```

**Management Services**

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

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

**WebUI**

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

**CLI**

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

**Hostname and Domain Name**

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

To configure the hostname and domain name on the device:

**WebUI**

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

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

**CLI**

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

**Date and Time**

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

To configure the date and time on the device:

**WebUI**

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

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

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

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

## Default Route

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

To configure the default route on the device:

### WebUI

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

```
IP Address/Netmask: 0.0.0.0/0.0.0.0
Next Hop
  Gateway: (select)
  Interface: ethernet0/2 (select)
  Gateway IP Address: ip_addr
```

### CLI

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

## Bridge Group Interfaces

The SSG 5 device is preconfigured with bridge group (bgroup) interfaces identified as bgroup0 through bgroup3. By default, the Ethernet interfaces ethernet0/2—ethernet0/6 are grouped together in bgroup0, which is bound to the Trust security zone.

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

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

---

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

---

To configure a bridge group with Ethernet and wireless interfaces:

### WebUI

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

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

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

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

### CLI

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

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

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

### WebUI

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

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

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

### CLI

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

## Backup Untrust Interface Configuration

The SSG 5 device lets you configure a backup interface for untrust failover. To set a backup interface for untrust failover:

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

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

---

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

---

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

#### WebUI

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

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

#### CLI

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

## Basic Wireless Configuration

---

This section describes how to configure the wireless interface on the SSG 5-WLAN device. Wireless networks consist of names referred to as Service Set Identifiers (SSIDs). Specifying SSIDs lets you have multiple wireless networks reside in the same location without interfering with each other. An SSID name can have a maximum of 32 characters. If a space is part of the SSID name string, then the string must be enclosed with quotation marks. Once the SSID name is set, more SSID attributes can be configured. To use the wireless local area network (WLAN) capabilities on the device, you must configure at least one SSID and bind it to a wireless interface.

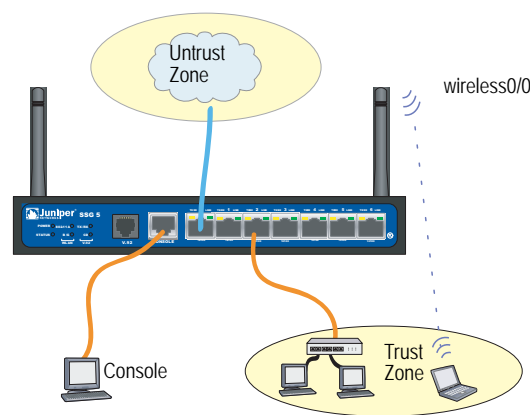
The SSG 5-WLAN device lets you create up to sixteen SSIDs, but only four of them can be used simultaneously. You can configure the device to use the four SSIDs on either one of the transceivers or split the use on both (for example, three SSIDs assigned to WLAN 0 and one SSID assigned to WLAN 1). Use the **set interface wireless\_interface wlan {0 | 1 | both}** command to set the radio transceivers on the SSG 5-WLAN device. Figure 10 shows the default configuration for the SSG 5-WLAN device.

Once you have set an SSID to the wireless0/0 interface, you can access the device using the default wireless0/0 interface IP address in the steps described in “Accessing the Device” on page 22. Figure 10 on page 32 shows the default configuration for the SSG 5-WLAN device.

**NOTE:** If you are operating the SSG 5-WLAN device in a country other than the United States, Japan, Canada, China, Taiwan, Korea, Israel, or Singapore, you must set the country code with the **set wlan country-code** command or set it on the Wireless > General Settings WebUI page before a WLAN connection can be established. This command sets the selectable channel range and the transmit power level.

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

**Figure 10: Default SSG 5-WLAN Configuration**



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

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

**Table 7: Wireless Authentication and Encryption Options**

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



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

To configure a wireless interface for basic connectivity:

### WebUI

1. Set the WLAN country code and IP address.

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

Country code: Select your code  
IP Address/Netmask: *ip\_add/netmask*

2. Set the SSID.

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

SSID:  
Authentication:  
Encryption:  
Wireless Interface Binding:

3. (Optional) set the WEP key.

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

4. Set the WLAN mode.

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

5. Activate wireless changes.

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

### CLI

1. Set the WLAN country code and IP address.

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

2. Set the SSID.

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

3. Set the WLAN mode.

```
set interface wireless_interface wlan both
```

4. Activate wireless changes.

```
save
exec wlan reactivate
```

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

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

#### **WebUI**

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

#### **CLI**

```
set interface bgroup_name port wireless_interface  
set interface bgroup_name port ethernet_interface
```

---

**NOTE:** *Bgroup\_name* can be bgroup0—bgroup3.

*Ethernet\_interface* can be ethernet0/0—ethernet0/6.

*Wireless\_interface* can be wireless0/0—wireless0/3.

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

---

## WAN Configuration

---

This section explains how to configure the following WAN interfaces:

- “ISDN Interface” on page 35
- “V.92 Modem Interface” on page 36

### **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 multilink Point-to-Point Protocol (PPP) 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, use the WebUI or CLI:

#### **WebUI**

Network > Interfaces > List > Edit (bri0/0): Enter or select the following, then click **OK**:

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

#### **CLI**

```
set interface bri0/0 dialer-enable
set interface bri0/0 primary-number "123456"
set interface bri0/0 encaps ppp
set interface bri0/0 ppp profile isdnprofile
save
```

To configure the ISDN interface as the backup interface, see “Backup Untrust Interface Configuration” on page 30.

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

## V.92 Modem Interface

The V.92 interface provides an internal analog modem to establish a PPP connection to a service provider. 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, use the WebUI or CLI:

### WebUI

Network > Interfaces > List > Edit (for serial0/0): Enter the following, then click **OK**:

Zone Name: untrust (select)

ISP: Enter the following, then click **OK**:

ISP Name: isp\_juniper  
 Primary Number: 1234567  
 Login Name: juniper  
 Login Password: juniper

Modem: Enter the following, then click **OK**:

Modem Name: mod1  
 Init String: AT&FS7=255S32=6  
 Active Modem setting  
 Inactivity Timeout: 20

### CLI

```
set interface serial0/0 zone untrust
set interface serial0/0 modem isp isp_juniper account login juniper password
juniper
set interface serial0/0 modem isp isp_juniper primary-number 1234567
set interface serial0/0 modem idle-time 20
set interface serial0/0 modem settings mod1 init-strings AT&FS7=255S32=6
set interface serial0/0 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 SSG 5 device is configured with a default policy that permits workstations in the Trust zone of your network to access any resource in the Untrust security zone, while outside computers are not allowed to access or start sessions with your workstations. You can configure policies that direct the device to permit outside computers to start specific kinds of sessions with your computers. For information about creating or modifying policies, refer to the *Concepts & Examples ScreenOS Reference Guide*.

The SSG 5 device provides various detection methods and defense mechanisms to combat probes and attacks aimed at compromising or harming a network or network resource:

- ScreenOS SCREEN options secure a zone by inspecting, and then allowing or denying, all connection attempts that require crossing an interface to that zone. For example, you can apply port-scan protection on the Untrust zone to stop a source from a remote network from trying to identify services to target for further attacks.
- The device applies firewall policies, which can contain content-filtering and Intrusion Detection and Prevention (IDP) components, to the traffic that passes the SCREEN filters from one zone to another. By default, no traffic is permitted to pass through the device from one zone to another. To permit traffic to cross the device from one zone to another, you must create a policy that overrides the default behavior.

To set ScreenOS SCREEN options for a zone:

### WebUI

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

### CLI

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

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

## Verifying External Connectivity

---

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

## Restarting the Device

---

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

The following sections describe two methods of restarting the device:

- “Restarting the Device with the CLI Reset Command” on page 38
- “Restarting the Device with the WebUI” on page 38

### ***Restarting the Device with the CLI Reset Command***

To restart the device with the CLI reset command:

1. Establish a console session with the device as described in “Using a Console Connection” on page 22 or “Using Telnet” on page 24.

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

The device prompts you for your login and password.

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

**reset**

The device prompts you to confirm the reset:

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

4. Enter **Y**.

The device restarts.

### ***Restarting the Device with the WebUI***

To restart the device with the WebUI:

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

The WebUI application displays the login prompt.

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

Configuration > Update > ScreenOS/Keys

4. Click **Reset**.

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

5. Click **OK**.

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

## Resetting the Device to Factory Defaults

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



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

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

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

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

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

### *Device Serial Number*

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

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

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

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

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

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

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

## ***unset all***

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

1. Start a Console session as described in “Using a Console Connection” on page 22, then log in.
2. At the command prompt, enter **unset all**. The following message is displayed:

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

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

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

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

## ***Reset Pinhole Button***

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

---

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

---

- Using the device status LEDs:

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

The Status LED blinks red.



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

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

■ Using the Console:

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

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

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

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

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

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



## Chapter 4

# Servicing the Device

This chapter describes service and maintenance procedures for an SSG 5 device. It contains the following sections:

- “Required Tools and Parts” on page 43
- “Upgrading Memory” on page 43

---

**NOTE:** For safety warnings and instructions, refer to the Juniper Networks *Security Products Safety Guide*. The instructions in the guide warn you about situations that could cause bodily injury. 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.

---

### Required Tools and Parts

---

To replace a component on the SSG 5 device, you need the following tools and parts:

- Electrostatic discharge (ESD) grounding wrist strap
- Number-2 phillips screwdriver

### Upgrading Memory

---

To upgrade the SSG 5 device from 128 MB to 256 MB of memory:

1. Attach an ESD grounding strap to your bare wrist and connect the strap to the ESD point on the chassis or to an outside ESD point if the device is disconnected from earth ground.
2. Unplug the AC cord from the power outlet.
3. Turn over the device so that its top is lying on a flat surface.
4. Use a phillips screwdriver to remove the screws from the memory-card cover. Keep the screws nearby for use when securing the cover later.
5. Remove the memory-card cover.

**Figure 11: Bottom of Device**



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

**Figure 12: Unlocking the Memory Module**



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

**Figure 13: Removing Module Slots**



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

Figure 14: Inserting the Memory Module



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



## Appendix A

# Specifications

This appendix provides general system specifications for the SSG 5 device. It contains the following sections:

- “Physical” on page 47
- “Electrical” on page 47
- “Environmental Tolerance” on page 48
- “Certifications” on page 48
- “RoHS and WEEE” on page 49
- “Connectors” on page 49

### Physical

---

Table 8 lists physical specifications for the SSG 5 device.

**Table 8: SSG 5 Physical Specifications**

Description	Value
Chassis dimensions	222.5 mm x 143.4 mm x 35 mm. With rubber feet, the system is 40 mm (1.6 inches) tall. (8.8 inches X 5.6 inches X 1.4 inches).
Device weight	960g (2.1 lbs).

### Electrical

---

Table 9 lists electrical specifications for the SSG 5 device.

**Table 9: SSG 5 Electrical Specifications**

Item	Specification
DC input voltage	12V
DC system current rating	4 Amps

## Environmental Tolerance

Table 10 lists environmental tolerance specifications for the SSG 5 device.

**Table 10: SSG 5 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 percent, noncondensing
Temperature	Normal operation ensured in temperature range of 32° F (0° C) to 104° F (40° C) Nonoperating storage temperature in shipping carton: -40° F (-40° C) to 158° F (70° C)

## Certifications

Table 11 lists certifications for the SSG 5 device.

**Table 11: SSG 5 Device Certifications**

Certification Type	Certification Name
Safety	CAN/CSA-C22.2 No. 60950-1-03/UL 60950-1 Third Edition, Safety of Information Technology Equipment EN 60950-1:2001+ A11, Safety of Information Technology Equipment IEC 60950-1:2001 First Edition, Safety of Information Technology Equipment
EMC Emissions	FCC Part 15 Class B (USA) EN 55022 Class B (Europe) AS 3548 Class B (Australia) VCCI Class B (Japan)
EMC Immunity	EN 55024 EN-61000-3-2 Power Line Harmonics EN-61000-3-3 Voltage Fluctuations and Flicker EN-61000-4-2 ESD EN-61000-4-3 Radiated Immunity EN-61000-4-4 EFT EN-61000-4-5 Surge EN-61000-4-6 Low Frequency Common Immunity EN-61000-4-11 Voltage Dips and Sags
ETSI	European Telecommunications Standards Institute (ETSI) EN-300386-2: Telecommunication Network Equipment. Electromagnetic Compatibility Requirements (equipment category Other than telecommunication centers)



## RoHS and WEEE

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

For more information about RoHS and WEEE compliance, visit:

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

## Connectors

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

**Figure 15: RJ-45 Connector Pin Numbering**

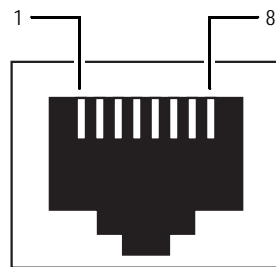


Table 12 lists the pinouts of the RJ-45 connectors for the Console and AUX ports.

**Table 12: Console and AUX RJ-45 Connector Pinouts**

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

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

**Figure 16: DB-9 Connector Pin Numbering**

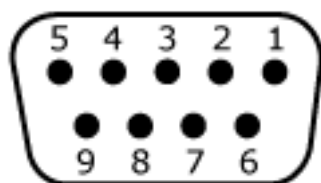


Table 13 lists the pinouts for the DB-9 adapter.

**Table 13: DB-9 Adapter Pinouts**

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

## Appendix B

# Initial Configuration Wizard

This appendix provides detailed information about the Initial Configuration Wizard (ICW) for an SSG 5 device.

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

This section describes the following ICW windows:

1. Rapid Deployment Window on page 52
2. Administrator Login Window on page 52
3. WLAN Access Point Window on page 53
4. Physical Interface Window on page 53
5. ISDN Interface Windows on page 54
6. V.92 Modem Interface Window on page 56
7. Eth0/0 Interface (Untrust Zone) Window on page 57
8. Eth0/1 Interface (DMZ Zone) Window on page 58
9. Bgroup0 Interface (Trust Zone) Window on page 58
10. Wireless0/0 Interface (Trust Zone) Window on page 60
11. Interface Summary Window on page 62
12. Physical Ethernet DHCP Interface Window on page 62
13. Wireless DHCP Interface Window on page 63
14. Confirmation Window on page 63

## 1. Rapid Deployment Window

Figure 17: Rapid Deployment Window



The image shows a 'Rapid Deployment Wizard' window. It has a blue title bar with the text 'Rapid Deployment Wizard'. Below the title bar, it says 'Welcome to the Rapid Deployment Wizard.' and 'Do you have a Rapid Deployment Configlet file?'. There are three radio button options: 
 

- ☒ No, use the Initial Configuration Wizard instead.
- ☐ Yes, use the following Rapid Deployment Configlet file: Below this is a text field 'Load Configlet from:' followed by a 'Browse...' button.
- ☐ No, skip the Wizard and go straight to the WebUI management session instead.

 At the bottom right, there are two buttons: 'Next >>' and 'Cancel'.

If your network uses Network and Security Manager (NSM), you can use a Rapid Deployment configlet to automatically configure the device. Obtain a configlet from your NSM administrator, select **Yes**, select **Load Configlet from:**, browse to the file location, then click **Next**. The configlet sets up the device for you, so you don't need to use the following steps to configure the device.

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

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

## 2. Administrator Login Window

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

Figure 18: Administrator Login Window



The image shows the 'Initial Configuration Wizard' window. It has a blue title bar with the text 'Initial Configuration Wizard'. Below the title bar, it says 'Enter the administrator's login name and password:'. There are three text input fields: 'Administrator Login Name:' (containing 'netscreen'), 'Password:' (containing '\*\*\*\*\*'), and 'Confirm Password:' (containing '\*\*\*\*\*'). Below these fields, there is a red note: 'Note: You cannot retrieve the login name and password if you lose it. Please make sure you have a copy of this information in a secure location.' Below the note, there is a checkbox labeled 'HTTP Redirect:' which is currently unchecked. Below the checkbox, there is another red note: 'Note: HTTP Redirect will redirect all HTTP traffic to HTTPS, i.e., HTTPS is only way to manage the device through Web browsers.' At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

### 3. WLAN Access Point Window

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

Figure 19: Country Code Window



The screenshot shows the 'Initial Configuration Wizard' window with the title bar in blue. The main text asks 'How do you want to configure the wireless access point?'. Below this, there are four configuration options, each with a dropdown menu: 'Regulatory Domain' is set to 'WORLD', 'Country Code' is set to 'NO\_COUNTRY\_SET', '2.4G Mode' is set to '802.11b/g', and '5G Mode' is set to '802.11a'. At the bottom, there is a checkbox labeled 'Configure wireless0/0 interface in trust zone.' which is checked. Below the checkbox are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

### 4. Physical Interface Window

On the interface-to-zone bindings screen, you set the interface to which you want to bind the Untrust security zone. Bgroup0 is prebound to the Trust security zone. Ethernet0/1 is bound to the DMZ security zone but is optional.

Figure 20: Physical Interface Window



The screenshot shows the 'Initial Configuration Wizard' window with the title bar in blue. The main text asks 'Please choose one interface for untrust, dmz and trust zone respectively.'. Below this, there are three configuration options, each with a dropdown menu: 'Untrust Zone' is set to 'eth0/0', 'DMZ Zone' is set to 'eth0/1', and 'Trust Zone' is set to 'bgroup0'. Below the dropdowns are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

After binding an interface to a zone, you can configure the interface. The configuration windows displayed after this point depend on which SSG 5 device you are using as part of your network. To continue configuring your device with the ICW, click **Next**.

## 5. ISDN Interface Windows

If you have one of the ISDN devices, a Physical Layer tab window similar to the following is displayed.

Figure 21: ISDN Physical Layer Tab Window

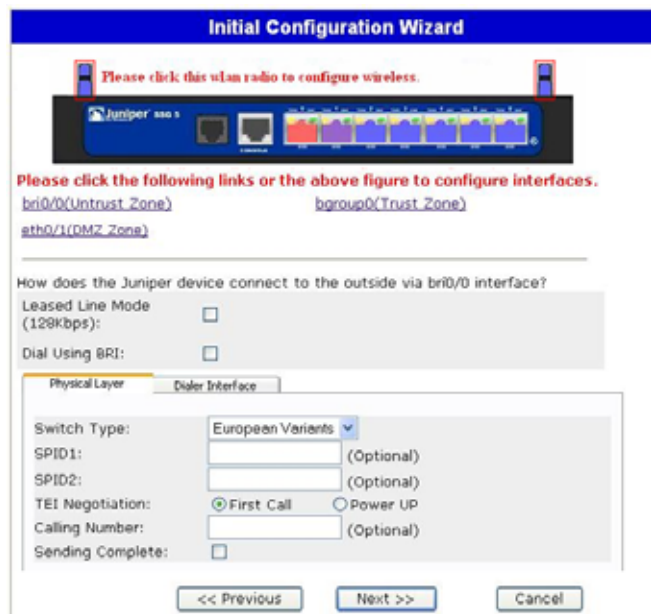


Table 14: Fields in ISDN Physical Layer Tab Window

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 NI1 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.
Sending Complete checkbox	Enables sending of complete information to outgoing setup message. Usually only used in Hong Kong and Taiwan.

If you have the ISDN device, you will see the Leased Line Mode and Dial Using BRI checkboxes. Selecting one or both checkbox(es) displays a window similar to the following:

Figure 22: Leased-Line and Dial Using BRI Tabs Window

The screenshot shows the 'Initial Configuration Wizard' window. At the top, there is a blue header bar with the title 'Initial Configuration Wizard'. Below the header, there is a red text box that says 'Please click this wlan radio to configure wireless.' with a red box around a WLAN radio icon. Below this, there is a diagram of a Juniper device with various ports. Below the diagram, there is a red text box that says 'Please click the following links or the above figure to configure interfaces.' with links for 'br0/0(Untrust\_Zone)', 'bgroup0(Trust\_Zone)', and 'eth0/1(DMZ\_Zone)'. Below the links, there is a question: 'How does the Juniper device connect to the outside via br0/0 interface?'. Below the question, there are two checkboxes: 'Leased Line Mode (128Kbps):' and 'Dial Using BRI:'. Below the checkboxes, there are two tabs: 'Physical Layer' and 'Dialer Interface'. The 'Dialer Interface' tab is selected. Below the tabs, there is a section titled 'Please create the PPP profile.' with fields for 'PPP Profile Name:', 'Authentication:' (with radio buttons for 'Any', 'CHAP', 'PAP', and 'None'), 'Local User:', 'Password:', and 'Static IP:' (with a checked checkbox). Below this section, there is a section for 'Interface Name:' (with a dropdown menu showing 'dialer 1'), 'Encapsulation Type:' (with radio buttons for 'ppp' and 'Multi-Link PPP'), 'Primary Number:', 'Alternative Number:' (with a note '(Optional)'), 'Dialer Pool:', 'Interface IP:', 'Netmask:', and 'Gateway:'. At the bottom of the window, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

Table 15: Fields in Leased-Line and Dial Using BRI Tabs Window

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

## 6. V.92 Modem Interface Window

If you have one of the V.92 devices, the following window is displayed:

Figure 23: V.92 Modem Interface Window

Table 16: Fields in V.92 Modem Interface Window

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 service provider
Primary Number	Specifies the phone number to access the service provider
Alternative Number (optional)	Specifies an alternative phone number to access the service provider if the primary number does not connect
Login Name	Sets the login name for the service provider account
Password	Sets the password for the login name



7. Eth0/0 Interface (Untrust Zone) Window

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

Figure 24: Eth0/0 Interface Window

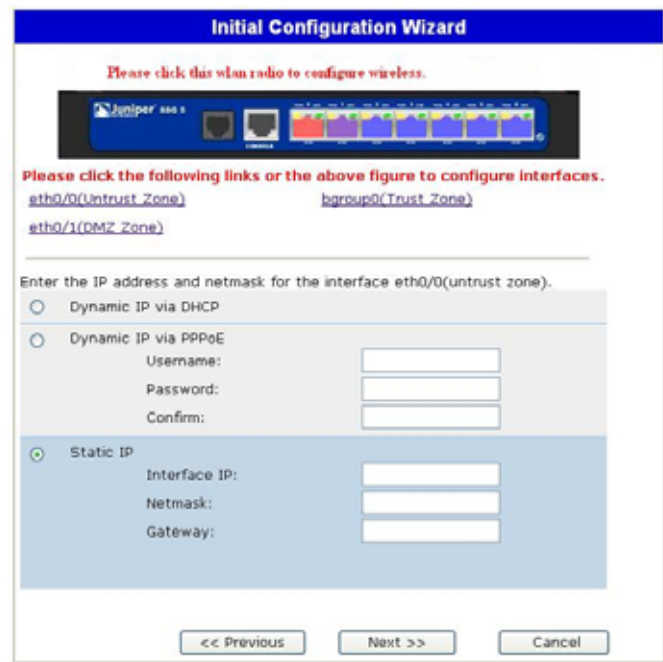


Table 17: Fields in Eth0/0 Interface Window

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

## 8. Eth0/1 Interface (DMZ Zone) Window

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

Figure 25: Eth0/1 Interface Window

Table 18: Fields in Ethernet0/1 Interface Window

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

## 9. Bgroup0 Interface (Trust Zone) Window

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

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

Figure 26: Bgroup0 Interface Window



Table 19: Fields in Bgroup0 Interface Window

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

## 10. Wireless0/0 Interface (Trust Zone) Window

If you have one of the SSG 5-WLAN devices, you must set a Service Set Identifier (SSID) before the wireless0/0 interface can be activated. For detailed instructions about configuring your wireless interface(s), refer to the *Concepts & Examples ScreenOS Reference Guide*.

Figure 27: Wireless0/0 Interface Window

The figure shows a screenshot of the 'Initial Configuration Wizard' window for configuring the wireless0/0 interface in the Trust Zone. At the top, there is a blue header bar with the title 'Initial Configuration Wizard'. Below the header, there is a red text prompt: 'Please click this wlan radio to configure wireless.' followed by a graphic of a device with various ports. Below this, there is another red text prompt: 'Please click the following links or the above figure to configure interfaces.' followed by four links: [eth0/0\(Untrust\\_Zone\)](#), [bgroup0\(Trust\\_Zone\)](#), [eth0/1\(DMZ\\_Zone\)](#), and [wireless0/0\(Trust\\_Zone\)](#). The main configuration area is titled 'How do you want to configure wireless0/0 interface(trust zone)?'. It contains several fields and options: 'Wlan Mode:' with a dropdown menu set to '2.4G(802.11b/g)'; 'SSID:' with an empty text box; 'Open' radio button selected, 'No Encryption' text; 'WPA-PSK' radio button selected, 'Passphrase(8~63 ASCII):' with an empty text box, 'Confirm:' with an empty text box, 'PSK(64 hexadecimal):' with an empty text box, 'Confirm:' with an empty text box; 'Encryption Type:' with 'Auto' selected, 'TKIP' unselected, and 'AES' unselected. At the bottom, there are 'Interface IP:' and 'Netmask:' fields with values '192.168.2.1' and '255.255.255.0' respectively. Navigation buttons at the bottom are '<< Previous', 'Next >>', and 'Cancel'.


Table 20: Fields in Wireless0/0 Interface Window

Field	Description
Wlan Mode	Sets the WLAN radio mode: <ul style="list-style-type: none"> <li>■ 5G (802.11a)</li> <li>■ 2.4G (802.11b/g)</li> <li>■ Both (802.11a/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 a wireless connection. You can choose to enter a HEX or an ASCII value for the PSK. A HEX PSK must be a 256-bit (64-text character) HEX value. An ASCII passphrase must be 8 to 63 text characters. You must select Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES) as the encryption type for this option, or select <b>Auto</b> to allow either option.</li> <li>■ WPA2 Pre-Shared Key.</li> <li>■ WPA Auto Pre-Shared Key.</li> </ul>
Interface IP	Sets the WLAN interface IP address.
Netmask	Sets the WLAN interface netmask.

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

## 11. Interface Summary Window

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



**Initial Configuration Wizard**

Before proceeding further, review the following interface settings.

ISDN Configuration:			
Switch Type:	etsi		
SPID1:	32546564565	SPID2:	23468458235
TEI Negotiation:	first call	Calling Number:	01023456789
T310 Value:	10	Sending Complete:	enabled
Leased Line Mode:	disabled	Dialer Enable:	disabled
PPP Profile:	myprofile	Authentication:	any
Local User:	myuser	Password:	mypwd
PPP Static IP:	enabled	Interface IP:	122.122.122.122

```

set interface br1/0 isdn switch-type etsi
set interface br1/0 isdn spid1 "32546564565"
set interface br1/0 isdn spid2 "23468458235"
set interface br1/0 isdn tei-negotiation first-call
set interface br1/0 isdn calling-number "01023456789"
set interface br1/0 isdn t310-value "10"
  
```

Click Next to enter other configuration

<< Previous    Next >>    Cancel

## 12. Physical Ethernet DHCP Interface Window

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



**Initial Configuration Wizard**

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

☐ Yes

IP Address Range Start:

End:

DNS Server 1 (optional):

DNS Server 2 (optional):

☒ No

<< Previous    Next >>    Cancel

### 13. Wireless DHCP Interface Window

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



**Initial Configuration Wizard**

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

### 14. Confirmation Window

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



**Initial Configuration Wizard**

Before proceeding further, review the following all device settings.

Admin Login:  Password:

Device is in NAT mode.

**ISDN Configuration:**

Switch Type:	etsi	SPID1:	32546564565	SPID2:	23488458235
TEI Negotiation:	first call	Calling Number:	01023456789		
T310 Value:	10	Sending Complete:	enabled		
Leased Line Mode:	disabled	Dialer Enable:	disabled		
PPP Profile:	myprofile	Authentication:	any		

```

set admin password "netscreen"
set interface bri1/0 isdn switch-type etsi
set interface bri1/0 isdn spid1 "32546564565"
set interface bri1/0 isdn spid2 "23488458235"
set interface bri1/0 isdn tei-negotiation first-call
set interface bri1/0 isdn calling-number "01023456789"
  
```

Click Next to save CLI into device.

<< Previous    Next >>    Cancel

After you click **Next**, the device reboots with the saved system configuration. The WebUI login prompt appears. For information on how to access the device using the WebUI, refer to “Using the WebUI” on page 24.





## Appendix C

# Country Code and Channel Information

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

- “Country Codes” on page 65
- “Wireless Channels” on page 65

### Country Codes

---

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

### Wireless Channels

---

**Table 21: Allowed Channels for All Countries (Page 1 of 2)**

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

**Table 21: Allowed Channels for All Countries (Page 2 of 2)**

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

# Index

<b>A</b>	
admin name and password.....	27
administrative access.....	27
<b>B</b>	
backup interface to Untrust zone .....	31
<b>C</b>	
configuration	
admin name and password.....	27
administrative access .....	27
backup untrust interface.....	30
bridge groups (bgroup).....	29
date and time .....	28
default route .....	29
host and domain name.....	28
management services .....	28
USB.....	14
WAN interfaces.....	35
wireless and Ethernet combined .....	34
wireless authentication and encryption.....	32
Console, managing with .....	22
<b>D</b>	
date and time.....	28
default IP addresses .....	25
<b>E</b>	
Ethernet port LEDs.....	12
<b>F</b>	
factory defaults, resetting to .....	39
<b>H</b>	
hostnames and domain names .....	28
<b>L</b>	
LEDs, Ethernet port.....	12
LINK LED .....	12
<b>M</b>	
management	
Console .....	22
services .....	28
Telnet.....	24
WebUI .....	24
managing	
through WebUI.....	38
memory upgrade procedure .....	43
<b>R</b>	
Reset/Reset Config button .....	40
resetting to factory defaults.....	39
restarting the device.....	38
<b>S</b>	
services, management .....	28
<b>T</b>	
Telnet, managing with .....	24
TX/RX LED .....	12
<b>U</b>	
Untrust zone, configuring backup interface .....	31
<b>W</b>	
WebUI, managing with .....	24
WebUI, using.....	38

